

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
16 août 2001 (16.08.2001)

PCT

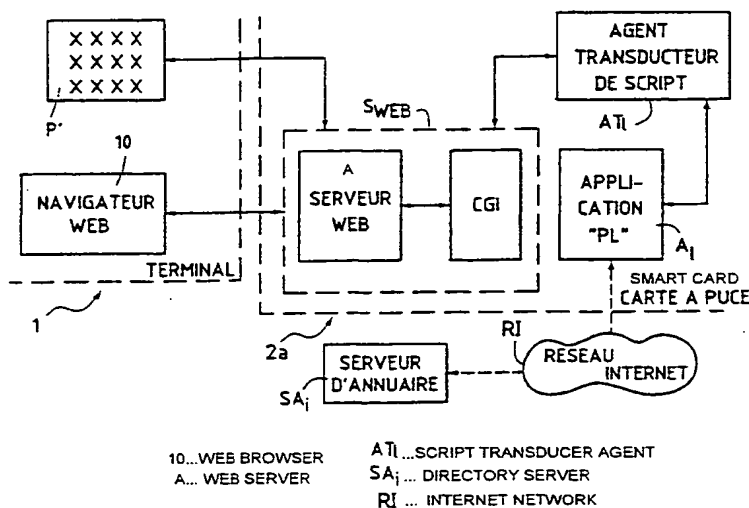
(10) Numéro de publication internationale
WO 01/60026 A1

- (51) Classification internationale des brevets⁷ : H04L 29/12, 29/06
- (72) Inventeur; et
(75) Inventeur/Déposant (*pour US seulement*) : URIEN, Pascal [FR/FR]; 4 rue du Ruisseau St Prix, F-78450 Villepreux (FR).
- (21) Numéro de la demande internationale : PCT/FR01/00396
- (22) Date de dépôt international : 9 février 2001 (09.02.2001)
- (74) Mandataire : CORLU, Bernard; Bull S.A., PC 58D20, 68, route de Versailles, F-78434 Louveciennes Cedex (FR).
- (25) Langue de dépôt : français
- (81) États désignés (*national*) : AU, CA, CN, JP, KR, SG, US.
- (26) Langue de publication : français
- (84) États désignés (*régional*) : brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- (30) Données relatives à la priorité : 00/01664 10 février 2000 (10.02.2000) FR
- (71) Déposant (*pour tous les États désignés sauf US*) : BULL CP8 [FR/FR]; 68, route de Versailles, Boîte Postale 45, F-78430 Louveciennes (FR).
- Publiée :
— avec rapport de recherche internationale

[Suite sur la page suivante]

(54) Title: METHOD FOR REGISTERING A USER ON AN INTERNET-TYPE NETWORK DIRECTORY SERVER AND/OR FOR LOCATING A USER ON SAID NETWORK, AND SMART CARD THEREFOR

(54) Titre : PROCEDE D'ENREGISTREMENT D'UN USAGER SUR UN SERVEUR D'ANNUAIRE D'UN RESEAU DE TYPE INTERNET ET/OU DE LOCALISATION D'UN USAGER SUR CE RESEAU, ET CARTE A PUCE POUR LA MISE EN OEUVRE DU PROCEDE



(57) Abstract: The invention concerns a method for registering a user on the directory and/or locating a cybernaut on an Internet-type network (RI), by interrogating a directory server (SA_i), so as to determine an IP address associated with said cybernaut. The method consists in using a smart card (2a) storing applications (A_i) each associated with a registering and/or locating protocol (PL). Subscriber profiles can be stored in the smart card (2a). Several different protocols can be stored, transforming the smart card (2a) into a multiple-directory database. The card (2a) is provided with WEB client/server and CGI functional capabilities, so as to be able to initiate transmissions in accordance with Internet protocols between directory server (SA_i) and the smart card (2a), and activate the applications (A_i) stored therein, for the process of registering and/or locating protocols (PL). The invention also concerns the related card.

[Suite sur la page suivante]

WO 01/60026 A1



— avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un procédé d'enregistrement d'un usager sur un serveur d'annuaire et/ou de localisation d'un internaute sur un réseau de type Internet (RI), par interrogation d'un serveur d'annuaire (SA_i), de manière à déterminer une adresse "IP" associée à cet internaute. Pour ce faire, on utilise une carte à puce (2a) stockant des applications (A_i) associées chacune à un protocole d'enregistrement et/ou de localisation ("PL"). Des profils d'abonnés peuvent être stockés dans la carte à puce (2a). Plusieurs protocoles différents peuvent être stockés, transformant la carte à puce (2a) en base de données multi-annuaire. La carte (2a) est dotée de fonctionnalités client/serveur "WEB" et "CGI", de manière à pouvoir initier des transmissions selon des protocoles Internet entre des serveurs d'annuaire (SA_i) et la carte à puce (2a), et activer les applications (A_i) stockées dans celle-ci, pour le déroulement des protocoles d'enregistrement et/ou localisation ("PL"). L'invention concerne aussi la carte associée.

Procédé d'enregistrement d'un usager sur un serveur d'annuaire d'un réseau de type Internet et/ou de localisation d'un usager sur ce réseau, et carte à puce pour la mise en œuvre du procédé

5 L'invention concerne un procédé d'enregistrement d'un usager sur un serveur d'annuaire d'un réseau notamment de type Internet et/ou de localisation d'un usager sur un tel réseau, à l'aide de cartes à puce connectées à des terminaux munis d'un lecteur de carte à puce.

L'invention concerne également une carte à puce pour la mise en
10 œuvre de ce procédé.

Dans le cadre de l'invention, le terme "réseau Internet" doit être compris dans son sens le plus général. Il concerne, outre le réseau Internet proprement dit, les réseaux privés d'entreprise ou similaires, du type dit "intranet", et les réseaux les prolongeant vers l'extérieur, du type dit
15 "extranet", et de façon générale tout réseau dans lequel les échanges de données s'effectuent selon un protocole du type Internet. Dans ce qui suit un tel réseau sera appelé de façon générique "réseau Internet".

De même, le terme "terminal" doit être compris dans un sens général. Le terminal précité peut être notamment constitué par un ordinateur personnel fonctionnant sous divers systèmes d'exploitation, tels WINDOWS
20 ou UNIX (tous deux étant des marques déposées). Il peut être aussi constitué par une station de travail, un ordinateur portable ou un terminal de carte dit dédié. Dans le cadre plus particulier de l'invention, il existe également des terminaux dédiés Internet, ne possédant qu'un minimum de
25 ressources informatiques propres, voire aucun moyens de stockage permanent, de type disque dur.

Il apparaît tout d'abord utile de rappeler brièvement les caractéristiques principales des protocoles de communication sur les réseaux.

30 L'architecture des réseaux de communication est décrite par diverses couches. A titre d'exemple, le standard "OSI" ("Open System

2

Interconnection"), défini par l' "ISO", comporte sept couches qui vont des couches dites basses (par exemple la couche dite "physique" qui concerne le support de transmission physique) aux couches dites hautes (par exemple la couche dite "d'application"), en passant par des couches intermédiaires, notamment la couche dite de "transport". Une couche donnée offre ses services à la couche qui lui est immédiatement supérieure et requiert de la couche qui lui immédiatement inférieure d'autres services, via des interfaces appropriées. Les couches communiquent à l'aide de primitives. Elles peuvent également communiquer avec des couches de même niveau. Dans certaines architectures, plusieurs couches peuvent être inexistantes.

Dans un environnement de type Internet, les couches sont au nombre de cinq, et de façon plus précise, en allant de la couche supérieure à la couche inférieure : la couche dite d'application ("http", "ftp", "e-mail", etc.), la couche dite de transport ("TCP"), la couche dite d'adressage de réseau ("IP"), la couche dite de liens de données ("PPP", "Slip", etc.) et la couche dite physique.

Dans l'art connu, un usager, que l'on appellera ci-après "internaute", utilise des terminaux Internet qui possèdent une adresse "IP" fixe, ou variable lorsque l'on a recours à un prestataire de service Internet, généralement connu sous le sigle anglo-saxon "ISP" (pour "Internet Service Provider").

Un premier inconvénient est constitué par le fait qu'une adresse "IP" n'est pas associée à un internaute, mais à un système informatique connecté au réseau Internet. Même dans le cas où le système informatique est doté d'une adresse fixe, il n'existe pas de correspondance *a priori* entre une adresse "IP" et une personne physique. Pour établir une telle relation l'internaute se connecte à des serveurs dits "IRC" (pour "Internet Relay Chat"). Ces serveurs associent à un identifiant de l'internaute, dit "UserID", son adresse "IP". L'identifiant est généralement constitué par son adresse courrier e-mel, ou "e-mail" selon la terminologie anglo-saxonne, mais un pseudonyme quelconque peut également être utilisé. Ci-après, les serveurs

3

"IRC" seront dénommés de façon plus générale "serveurs d'annuaires", que l'on appellera simplement "SA".

Cette association n'est généralement pas authentifiée de telle sorte que le service (généralement gratuit) puisse être utilisé de la manière la plus
5 commode possible. Cette disposition n'est cependant pas exempte d'inconvénients, en particulier pour des applications dites "sensibles".

Une des premières contraintes rencontrées est donc la localisation d'un internaute dans le réseau Internet, c'est à dire l'établissement d'une correspondance entre un identifiant fixe et une adresse "IP".

10 Cependant la localisation d'un internaute sur le réseau Internet, c'est-à-dire l'établissement de la correspondance précitée, présuppose que celui-ci ait été au préalable enregistré dans le serveur d'annuaire "SA".

L'adresse d'un internaute dans le réseau Internet est donc constituée du couple : "Adresse SA" - "UserID". De façon usuelle, par
15 "abonné", on entend une entité "physique". Par extension, il peut s'agir d'une "fonction". Cependant, ci-après, on donnera à "abonné" son sens commun, sans que cela soit limitatif en quoi que ce soit de la portée de l'invention.

De façon pratique, un internaute indique sa localisation dans le réseau Internet par un acte volontaire en fournissant au serveur (annuaire)
20 son adresse "IP" actuelle à l'aide d'un protocole d'enregistrement que l'on appellera ci-après "PE".

Cette opération implique que le terminal possède un logiciel spécifique (ou application) délivré par le fournisseur du service, et personnalisé avec un profil d'abonné particulier, que l'on appellera "PA" ci-
25 après. Ce profil "PA" permet d'identifier de façon plus complète un abonné (ou internaute), en sus de son identifiant de base "UserID".

On désigne généralement par "Profil d'Abonné" ("PA") l'ensemble des informations qui sont fournies au serveur d'annuaire "SA" lors de l'enregistrement de l'abonné (internaute), et par exemple :

- 30
- l'adresse du "Serveur d'Annuaire" ("SA") ;
 - l'identifiant de l'abonné ("UserID") ;

- les abonnés (identifiés par leurs "UserID") avec lesquels l'utilisateur accepte d'entrer en communication ou auxquels il désire notifier sa localisation dans le réseau ; et

5 - les informations qu'il accepte de rendre publiques sur le serveur d'annuaire (par exemple : nom, nationalité, contacts recherchés, etc.). ;

Pour joindre un correspondant à travers le réseau Internet, ce correspondant étant dûment enregistré, il est nécessaire de connaître son adresse "IP". Cette information est obtenue à l'aide d'un serveur d'annuaire
10 ("SA") et d'un protocole de localisation ("PL").

On doit noter que le profil d'abonné "PA" est, par nature, spécifique à l'abonné, mais peut dépendre aussi des caractéristiques du serveur d'annuaire, notamment du type et de la nature des informations qui doivent lui être fournies ou qu'il peut accepter.

15 On doit noter enfin que le protocole "PL" est, comme le protocole "PE", de type dit propriétaire, puisqu'il adresse un serveur d'annuaire *a priori* non standardisé ou répondant à des normes universellement reconnues.

Ces deux caractéristiques constituent des inconvénients supplémentaires.

20 En résumé de ce qui vient d'être rappelé, pour qu'un premier internaute puisse localiser d'autres internautes et puisse être localisé par ceux-ci, il est nécessaire que le terminal qu'il utilise stocke des logiciels spécifiques permettant de mettre en œuvre les protocoles "PE" et "PL". Il peut également être nécessaire qu'il stocke des données afférentes à son
25 profil d'abonné "PA". Cette remarque s'applique de façon similaire aux terminaux des autres internautes.

En d'autres termes, le terminal utilisé par un abonné quelconque est également spécifique, en ce sens que, si cet abonné désire changer de terminal, il doit retrouver sur le nouveau terminal utilisé, au moins le ou les
30 logiciels associés au protocole "PL", en admettant qu'il ait procédé à une phase préliminaire d'enregistrement sur le premier terminal, en faisant appel

5

au protocole "PE" et en fournissant son profil "PA" au serveur d'annuaire "SA". En effet, la présence du protocole "PL" sera nécessaire pour adresser le serveur d'annuaire et avoir accès aux données enregistrées dans celui-ci, notamment les adresses "IP" des correspondants recherchés et leurs profils "SA".

Il serait donc intéressant d'utiliser des terminaux banalisés pour effectuer les opérations d'enregistrement et, surtout, de localisation d'internautes sur le réseau Internet, ce qui permettrait d'accéder de façon commode au concept appelé "nomadisme".

Les logiciels associés aux protocoles précités, "PE" et "PL" ne nécessitent pas habituellement de disposer d'une grande quantité de mémoire. Il en est de même des données de profil "PA". On pourrait donc penser les enregistrer dans les circuits de mémoire d'une carte à puce, ce que permet la technologie actuelle.

Cependant, on se heurte à une double difficulté technique, comme il va l'être montré ci-après, ce qui interdit toute communication directe entre le réseau Internet et une carte à puce.

On va tout d'abord rappeler brièvement l'architecture générale d'un système d'application à base de carte à puce, relié à un réseau Internet, par référence aux figures 1A et 1B.

Un système d'application à base de carte à puce comporte généralement les éléments principaux suivants :

- une carte à puce ;
- un système hôte constituant le terminal précité ;
- un réseau de communication, à savoir le réseau Internet dans l'application préférée ;
- et un serveur d'application connecté au réseau Internet.

La figure 1A illustre schématiquement un exemple d'architecture de ce type. Le terminal 1, par exemple un ordinateur individuel, comporte un lecteur 3 de carte à puce 2. Ce lecteur 3 peut être ou non physiquement intégré dans le terminal 1. La carte à puce 2 comporte un circuit intégré

6

dont des connexions d'entrées-sorties affleurent en surface de son support pour autoriser une alimentation en énergie électrique et des communications avec le terminal 1. Ce dernier comprend des circuits d'accès 11 au réseau Internet *RI*. Ces circuits peuvent être constitués par un modem pour se
5 connecter à une ligne téléphonique commutée ou à une voie de communication à plus haut débit : réseau numérique à intégration de services ("RNIS"), câble ou liaisons par satellite, etc. Les circuits 11 permettent de se connecter au réseau Internet *RI*, directement ou via un prestataire de services Internet ("Internet Service Provider" ou "ISP", selon la
10 terminologie anglo-saxonne). On peut également avoir recours à un système intermédiaire tel qu'un "proxy" ou un système d'isolation dit "firewall" ("pare-feu" ou encore appelé "garde barrière").

Le terminal 1 comprend naturellement tous les circuits et organes nécessaires à son bon fonctionnement, et qui n'ont pas été représentés
15 dans un but de simplification du dessin : unité centrale, mémoires vive et fixe, mémoire de masse à disque magnétique, lecteur de disquette et/ou de CédéRom, etc.

Habituellement, le terminal 1 est aussi relié à des périphériques classiques, intégrés ou non, tels un écran de visualisation 5, un clavier 6a et
20 une souris 6b, etc.

Le terminal 1 peut être mis en communication avec des serveurs ou tous systèmes informatiques connectés au réseau *RI*, dont un seul, 4, est illustré sur la figure 1A. Les circuits d'accès 11 mettent le terminal 1 en communication avec les serveurs 4 grâce à un logiciel particulier 10, appelé
25 navigateur "WEB", ou "browser" selon la terminologie anglo-saxonne. Celui-ci permet d'accéder à diverses applications ou fichiers de données répartis sur l'ensemble du réseau *RI*, généralement selon un mode "client-serveur".

Habituellement, les communications sur les réseaux s'effectuent conformément à des protocoles répondant à des standards comprenant
30 plusieurs couches logicielles superposées. Dans le cas d'un réseau *RI* de type Internet, les communications s'effectuent selon des protocoles

7

spécifiques à ce type de communications, qui seront détaillés ci-après, mais qui comprennent également plusieurs couches logicielles. Le protocole de communication est choisi en fonction de l'application plus particulièrement visée : interrogation de pages "WEB", transferts de fichiers, courrier électronique (e-mel, ou "e-mail" selon la terminologie anglo-saxonne), forums ou "news", etc.

L'architecture logique du système comprenant un terminal, un lecteur de carte à puce et une carte à puce, est représentée schématiquement par la figure 1C. Elle est décrite par la norme ISO 7816, qui elle-même comportent plusieurs sous-ensembles :

- ISO 7816-1 et 7816-2, en ce qui concerne les dimensions et le marquage des cartes ;
- ISO 7816-3, en ce qui concerne le transfert de données entre le terminal et la carte à puce ; et
- ISO 7816-4, en ce qui concerne la structure du jeu d'ordres et le format des commandes.

Sur la figure 1B, du côté terminal 1, on n'a représenté que les couches répondant à la norme ISO 7816-3, référencées 101, et un gestionnaire d'ordres "APDU" (norme ISO 7816-4), référencé 102. Du côté carte à puce 2, les couches répondant à la norme ISO 7816-3 sont référencées 200 et le gestionnaire d'ordres "ADPU" (norme ISO 7816-4) est référencé 201. Les applications sont référencées $A_1, \dots, A_i, \dots, A_n$; n étant le nombre maximum d'applications présentes sur la carte à puce 2.

Une application, A_i , présente dans la carte à puce 2, dialogue avec le terminal 1 au moyen d'un jeu d'ordres. Ce jeu présente typiquement des ordres d'écriture et des ordres de lecture. Le format des ordres est connu sous l'abréviation anglo-saxonne de "APDU" (pour "Application Protocol Data Unit"). Il est défini par la norme ISO 7816-4 précitée. Une "APDU" de commande est notée "APDU.command" et une "APDU" de réponse est notée "APDU.response". Les "APDU" sont échangées entre le lecteur de

8

carte et la carte à puce au moyen d'un protocole spécifié par la norme ISO 7816-3 précitée (par exemple en mode caractère : T=0 ; ou en mode bloc : T=1).

5 Lorsque la carte à puce 2 inclut plusieurs applications distinctes, comme illustré sur la figure 1B, on parle de carte multi-applicative. Cependant, le terminal 1 ne dialogue qu'avec une seule application à la fois.

La sélection d'une application particulière A_i est obtenue à l'aide d'une "APDU" du type sélection ("SELECT"). Une fois ce choix effectué, les "APDU" qui le suivent sont acheminés vers cette application. Une "APDU
10 SELECT" nouvelle a pour effet d'abandonner l'application en cours et d'en choisir une autre. Le sous-ensemble logiciel gestionnaire des "APDU" 201 permet de choisir une application particulière A_i dans la carte à puce 2, de mémoriser l'application ainsi choisie, et de transmettre et/ou recevoir des "APDU" vers et depuis cette application.

15 En résumé de ce qui vient d'être décrit, la sélection d'une application A_i et le dialogue avec celle-ci s'effectuent par échanges d'ordres "APDU". On suppose que les applications A_i sont des applications conventionnelles, que l'on appellera ci-après "GCA" (pour "Generic Card Application" ou application de carte générique).

20 Ces rappels étant effectués, il est à noter que la carte à puce 2 ne peut communiquer directement avec les navigateurs standards du commerce 10, sauf à modifier le code de ces derniers.

En outre, et surtout, les cartes à puce actuelles, qui par ailleurs sont conformes aux standards et normes rappelés ci-dessus, ont une
25 configuration matérielle et logicielle qui ne permet pas non plus de communiquer directement avec le réseau Internet. En particulier, elles ne peuvent recevoir et transmettre des paquets de données, selon l'un ou l'autre des protocoles utilisés sur ce type de réseau. Il est donc nécessaire de prévoir une pièce de logiciel additionnelle, implantée dans le terminal 1,
30 généralement sous la forme de ce qui est appelé un "plug-in", selon la

terminologie anglo-saxonne. Cette pièce de logiciel, qui porte la référence 12 sur la figure 1A, effectue l'interface entre le navigateur 10 et la carte 2, plus précisément les circuits électroniques 20 de cette carte 2.

L'invention vise à pallier les inconvénients des procédés et
5 dispositifs de l'art connu, et dont certains viennent d'être rappelés, tout en répondant aux besoins qui se font sentir.

Selon un mode de réalisation avantageux de l'invention, les applications nécessaires à la mise en œuvre des protocoles d'enregistrement ("PE") et de localisation ("PL"), ainsi que les données
10 caractérisant le profil d'abonné ("PA") sont des fichiers stockés, en tout ou partie, dans des mémoires d'une carte à puce, les fichiers de type exécutable étant des applications standards du type "GCA" précité.

Selon l'invention, la carte à puce se comporte comme un serveur/client de type "WEB" pour le terminal qui lui est associé.

15 Pour ce faire, on prévoit une couche de logiciel de communication spécifique dans la carte à puce et son pendant dans le terminal. Le terme "spécifique" doit être entendu comme spécifique au procédé de l'invention. En effet, ces couches de communications, dites spécifiques, sont banalisées quelle que soit l'application considérée. En particulier, elles sont
20 indépendantes des applications nécessaires à la mise en œuvre des protocoles "PE" et "PL". Elles n'interviennent que dans le processus d'échanges de données bidirectionnels entre la carte à puce et le terminal, d'une part, et la carte à puce et le réseau, d'autre part.

Les couches logicielles de communication spécifiques comprennent
25 notamment des composants logiciels, dits "agents intelligents", permettant en particulier des conversions de protocoles. Les agents intelligents seront appelés ci-après plus simplement "agents". Il existe des agents appareillés dans les couches de communication spécifiques respectives associées au terminal et à la carte à puce. Selon le procédé de l'invention, il s'établit des
30 sessions entre agents appareillés.

10

Avantageusement, le procédé de l'invention rend possible l'activation d'applications de type conventionnel, c'est-à-dire du type "CGA" précité, localisées dans une carte à puce, sans devoir les modifier en quoi que ce soit.

- 5 Pour ce faire, on prévoit un ou plusieurs agents intelligents particuliers dits traducteurs de script, qui reçoivent des requêtes d'un navigateur et les traduisent en ordres "APDU" compréhensibles par l'application de type "CGA". De ce fait, on implante dans la carte à puce une fonction similaire à celle connue par ailleurs sous la dénomination "CGI" dans les serveurs "WEB" classiques. Cette fonction permet de mettre en œuvre une application dans la carte à puce par un protocole Internet de type "HTTP".

- Ces diverses dispositions permettent à la carte à puce, et plus précisément aux applications présentes dans celle-ci, de communiquer directement avec un serveur éloigné connecté au réseau Internet par la mise en œuvre de protocoles de type Internet. La fonctionnalité "CGI" offerte par la carte à puce permet pour sa part l'accès aux applications associées aux protocoles "PE" et "PL" et leur exécution, sans nécessiter la présence d'applications de type propriétaire dans le terminal. Seul un navigateur, avantageusement de type standard du commerce, est nécessaire.

Dans une variante préférée de réalisation de l'invention, on stocke dans la carte à puce plusieurs jeux composés d'applications associées à des protocoles "PE" et "PL" et/ou de profils d'abonnés "PA" distincts.

- Cette disposition avantageuse permet, d'une part, d'enregistrer plusieurs profils d'abonné "PA" distincts ou plusieurs occurrences distinctes d'un même profil d'abonné "PA" sur un même serveur d'annuaire "SA", et de localiser ces entités en les associant à des adresses "IP" uniques. Elle permet, d'autre part, de pouvoir adresser plusieurs serveurs d'annuaire "SA", avec un même et/ou plusieurs profils d'abonnés "PA" distincts. La carte à puce présente alors une fonctionnalité de base de données multi-annuaire.

L'invention a donc pour objet principal un procédé de mise en relation d'un premier usager avec au moins un serveur d'annuaire, en vue de son enregistrement et/ou de la localisation d'au moins un deuxième usager sur un réseau notamment de type Internet, ladite mise en relation s'effectuant

5 par l'intermédiaire d'un terminal muni d'un lecteur de carte à puce et d'au moins une pièce de logiciel dite d'enregistrement et/ou de localisation, ledit terminal étant connecté à chacun desdits serveurs d'annuaire via ledit réseau de type Internet et communiquant avec ladite carte à puce selon un premier protocole déterminé, caractérisé en ce qu'au moins l'une desdites

10 pièces de logiciel est stockée dans ladite carte à puce ; en ce que cette carte à puce comprenant une première pièce de logiciel, formant une couche protocolaire de communication spécifique, et ledit terminal comprenant une seconde pièce de logiciel, formant une couche protocolaire de communication spécifique, lesdites première et seconde pièces de logiciel

15 comprennent en outre au moins une paire de premières entités logicielles appariées, chacune desdites entités coopérant l'une avec l'autre de manière à permettre l'établissement d'une session d'échanges de données bidirectionnels entre au moins ledit terminal et ladite carte à puce, et/ou ledit réseau de type Internet, de manière à ce que ladite carte à puce offre la

20 fonctionnalité d'un client/serveur "WEB" ; en ce que ladite carte à puce comprend au moins une deuxième entité logicielle coopérant avec ladite seconde pièce de logiciel spécifique pour que ladite carte à puce offre une fonctionnalité d'interface passerelle dite "CGI" :

et en ce qu'il comprend au moins les étapes suivantes :

- 25 1/ ouverture d'une première séquence d'échanges de données entre au moins ledit terminal et ladite carte à puce, pour la transmission d'une requête pour que ledit navigateur de type "WEB" récupère des données permettant de sélectionner et d'activer une desdites pièces de logiciel propriétaire, en vue de la sélection d'un desdits serveurs d'annuaire ;

12

- 2/ ouverture d'une deuxième séquence d'échanges de données entre ladite carte à puce et ledit terminal pour lui transmettre lesdites données ;
- 5 3/ ouverture d'une troisième séquence d'échanges de données entre ledit terminal et ladite carte à puce pour transmettre des données de sélection et des paramètres optionnels, lesdites données et lesdits paramètres optionnels comportant une référence à une desdites pièces de logiciel d'enregistrement et/ou de localisation ;
- 10 4/ mise en œuvre de ladite fonctionnalité "CGI" et exécution de ladite pièce de logiciel d'enregistrement et/ou de localisation ; et
- 5/ en résultat de ladite exécution, ouverture d'une quatrième séquence d'échanges de données entre ladite carte à puce et un desdits serveurs d'annuaire, sélectionné par lesdites données de sélection, de manière à transmettre une requête pour la réalisation
- 15 d'une opération déterminée d'enregistrement ou de localisation.

L'invention a également pour objet une carte à puce pour la mise en œuvre de ce procédé.

Un mode préféré, mais non limitatif, de réalisation de l'invention va maintenant être décrit de façon plus détaillée en se référant aux dessins annexés, parmi lesquels :

20

- les figures 1A et 1B illustrent les architectures matérielle et logique, respectivement, d'un exemple de système d'application à base de carte à puce connecté à un réseau Internet selon l'art connu ;
- 25 - la figure 2 illustre schématiquement un exemple de système d'application à base de carte à puce selon l'invention, cette dernière agissant en tant que client/serveur "WEB", selon un aspect de l'invention ;
- la figure 3 est un diagramme d'états d'une session entre des
- 30 entités logicielles dites agents intelligents, selon un aspect de l'invention ;

13

- la figure 4 illustre de façon simplifiée l'architecture logique d'un système selon l'invention, dans lequel la carte à puce comprend des agents intelligents ;
- 5 - la figure 5 illustre de façon simplifiée l'architecture logique d'un système selon un autre aspect de l'invention selon lequel la carte à puce comprend des agents intelligents traducteurs de scripts, de manière à implanter une fonction dite "CGI" ;
- la figure 6A illustre schématiquement une première étape de la phase d'enregistrement d'un internaute sur un serveur d'annuaire ;
- 10 - les figures 6B et 6C illustrent des exemples de formulaires "HTLM" utilisables pour cette phase d'enregistrement ;
- la figure 6D illustre schématiquement les principales étapes de la phase d'enregistrement d'un internaute sur un serveur d'annuaire ;
- la figure 6E illustre schématiquement les principales étapes de la phase d'enregistrement d'un internaute plusieurs serveurs d'annuaire ;
- 15 - la figure 7 illustre schématiquement les principales étapes de la phase de localisation d'un internaute sur le réseau Internet par interrogation d'un serveur d'annuaire ; et
- 20 - la figure 8 illustre schématiquement une architecture à carte à puce selon l'invention présentant une fonctionnalité de base de données multi-annuaire portable.

La figure 2 illustre schématiquement un exemple de système d'application à base de carte à puce selon un premier aspect de l'invention, permettant à cette dernière d'agir en tant que client/serveur "WEB".

A l'exception de couches logicielles de protocole de communication spécifiques, référencées 13 et 23a, respectivement implantées dans le terminal 1 et la carte à puce 2a, les autres éléments, matériels ou logiciels, sont communs à l'art connu, notamment à ce qui a été décrit en regard des figures 1A et 1B, et il n'y a pas lieu de les re-décrire de façon détaillée.

14

Le terminal 1 comprend des circuits 11 d'accès au réseau *R/I*, constitués par exemple d'un modem. Ces circuits regroupent les couches logicielles inférieures, C₁ et C₂, qui correspondent aux couches "physique" et de "lien de données".

- 5 On a également représenté les couches supérieures, C₃ et C₄, qui correspondent aux couches "d'adressage de réseau" ("IP", dans le cas d'Internet) et de "transport" ("TCP"). La couche supérieure d'application ("http", "ftp", "e-mail", etc.) n'a pas été représentée.

- L'interface entre les couches inférieures, C₁ et C₂, et les couches
10 supérieures, C₃ et C₄, est constituée par une couche logicielle généralement appelée "driver couches basses". Les couches supérieures, C₃ et C₄, s'appuient sur cette interface et sont mises en œuvre par l'intermédiaire de bibliothèques de fonctions spécifiques ou bibliothèques réseau 14, avec lesquelles elles correspondent. Dans le cas du réseau
15 Internet, "TCP/IP" est mis en œuvre au moyen de bibliothèques dites de "sockets".

- Cette organisation permet à un navigateur 10 de poser des requêtes vers un serveur 4, pour la consultation de pages "WEB" (protocole "HTTP"), pour le transfert de fichiers (protocole "FTP") ou l'envoi de courrier
20 électronique (protocole "e-mail"), ce de façon tout à fait classique en soi.

- Le terminal 1 comprend également un lecteur de carte 3, intégré ou non. Pour communiquer avec la carte à puce 2a, le lecteur de carte 30 englobe également deux couches basses, CC₁ (couche physique) et CC₂ (couche de lien de données), jouant un rôle similaire aux couches C₁ et C₂.
25 Les interfaces logicielles avec les couches CC₁ et CC₂ sont décrites, par exemple, par la spécification "PC/SC" ("part 6, service provider"). Les couches elles-mêmes, CC₁ et CC₂, sont notamment décrites par les normes ISO 7816-1 à 7816-4, comme il a été rappelé.

- Une couche logicielle supplémentaire 16 forme interface entre les
30 couches applicatives (non représentées) et les couches inférieures, CC₁ et

15

CC2. La fonction principale dévolue à cette couche 16 est une fonction de multiplexage/démultiplexage.

Les communications avec la carte à puce 2a s'effectuent selon un paradigme similaire à celui utilisé pour la manipulation de fichiers dans un système d'exploitation du type "UNIX" (marque déposée) : OUVRI
5 ("OPEN"), LIRE ("READ"), ECRIRE ("WRITE"), FERMER ("CLOSE"), etc.

Du côté de la carte à puce 2a, on retrouve une organisation similaire, à savoir la présence de deux couches basses, référencées CCa1 (couche physique) et CCa2 (couche de lien de données), ainsi qu'une couche
10 d'interface 26a, tout à fait similaire à la couche 16.

Selon l'invention, on prévoit, de part et d'autre, c'est-à-dire dans le terminal 1 et dans la carte à puce 2a, deux couches de protocoles spécifiques : 13 et 23a, respectivement.

Dans le terminal 1, la couche spécifique 13 s'interface aux "drivers couches basses" 15, aux bibliothèques 14 des couches réseau, C3 et C4, et aux couches protocolaires du lecteur de carte 3, c'est-à-dire les couches inférieures, CC1 et CC2, via la couche de multiplexage 16. La couche spécifique 13 permet le transfert de paquets réseaux de et vers la carte à puce 2a. En outre, elle adapte les applications existantes telles le navigateur Internet 10, le courrier électronique, etc., pour des utilisations mettant en
20 œuvre la carte à puce 2a.

Du côté de la carte à puce 2a, on retrouve une organisation tout à fait similaire constituée par une instance supplémentaire de la couche spécifique, référencée 23a, pendant de la couche 13.

25 De façon plus précise, les couches spécifiques, 13 et 23a, sont subdivisées en trois éléments logiciels principaux :

- un module, 130 ou 230a, de transfert de blocs d'informations entre les couches 13 et 23a, via les couches conventionnelles CC1, CC2, CCa1 et CCa2 ;

16

- une ou plusieurs pièces de logiciel, dites "agents intelligents", 132 ou 232a, qui réalisent, par exemple, des fonctions de conversion de protocoles ;

5 - et un module de gestion de la configuration spécifique, 131 et 231a, respectivement ; module qui peut être assimilé à un agent intelligent particulier.

Pour simplifier, on appellera ci-après les agents intelligents, "agents", comme il a été précédemment indiqué.

10 On retrouve donc, dans le terminal 1 et la carte à puce 2a, une pile protocolaire de communication entre les deux entités.

Les couches de niveau deux (couches de lien de données), CC₂ et CCa₂, assurent l'échange entre la carte à puce 2a et le terminal 1. Ces couches sont responsables de la détection et l'éventuelle correction d'erreurs de transmission. Différents protocoles sont utilisables, et à titre 15 d'exemples non exhaustifs les suivants :

- la recommandation ETSI GSM 11.11 ;
- le protocole défini par la norme ISO 7816-3, en mode caractère T=0 ;

- le protocole défini par la norme ISO 7816-3, en mode bloc T=1 20 ;

- ou le protocole défini par la norme ISO 3309, en mode trame "HDLC" (pour "High-Level Data Link Control procedure" ou procédure de commande de liaison à haut niveau).

25 Dans le cadre de l'invention, on utilisera de préférence le protocole ISO 7816-3, en mode bloc.

De façon connue en soi, à chaque couche de protocole, il est associé un certain nombre de primitives qui permettent les échanges de données entre couches de même niveau et d'une couche à l'autre. A titre d'exemple, les primitives associées à la couche de niveau deux sont du type

17

"demande de données" ("*Data.request*") et "envoi de données" par la carte ("*Data.response*"), ainsi que "confirmation de données" ("*Data.confirm*"), etc.

De façon plus spécifique, les couches 13 et 23a sont chargées du dialogue entre la carte à puce 2a et l'hôte, c'est-à-dire le terminal 1. Ces
5 couches permettent l'échange d'informations entre un utilisateur (non représenté) du terminal 1 et la carte à puce 2a, par exemple via des menus déroulants sous la forme d'hypertexte au format "HTML". Elles permettent aussi la mise en place d'une configuration adaptée pour l'émission et/ou la réception de paquets de données.

10 Comme il a été indiqué ci-dessus, les couches comprennent trois entités distinctes.

La première couche, 130 ou 230a, est essentiellement constituée par un multiplexeur logiciel. Elle permet l'échange d'informations entre la carte à puce 2a et le terminal hôte 1, sous la forme d'unités de données de
15 protocole. Elle joue un rôle similaire à celui d'un commutateur de paquets de données. Ces unités sont émises ou reçues via la couche de niveau deux (couche de liens de données). Ce protocole particulier de communication permet de mettre en communications au moins une paire d' "agents". Le premier agent de chaque paire, 132, est situé dans la couche 13, côté
20 terminal 1, le second, 232a, est situé dans la couche 23a, côté carte à puce 2a. Une liaison entre deux "agents" est associée à une session, que l'on pourra appeler "*S-Agent*". Une session est un échange de données bidirectionnel entre ces deux agents. Si l'une ou l'autre des couches, 13 et 23a, comporte plusieurs agents, les agents d'une même couche peuvent
25 aussi établir de sessions entre eux et/ou avec les modules 131 et 231a, qui constituent des agents particuliers.

De façon plus précise, un agent est une entité logicielle autonome qui peut réaliser tout ou partie de fonctions des couches de niveau trois et quatre, en fonction de la configuration mise en œuvre par le terminal 1.

18

Les agents sont associés à des propriétés ou attributs particuliers. Pour fixer les idées, et à titre d'exemple non limitatif, les six propriétés suivantes sont associées aux agents :

- "hôte" : agent localisé dans le terminal ;
- 5 - "carte" : agent localisé dans la carte à puce ;
- "local" : agent ne communiquant pas avec le réseau ;
- "réseau" : agent communiquant avec le réseau (côté terminal) ;
- "client" : agent qui initialise une session ;
- "serveur" : agent qui reçoit une demande de session.

10 Un agent particulier est identifié par une référence, par exemple un nombre entier de 16 bits (c'est-à-dire compris entre 0 et 65535). Le bit de poids fort ($b_{15} = 1$) indique si la référence est locale (communications locales à la carte à puce ou au terminal) ou distante ($b_{15} = 0$).

15 Il existe deux grandes catégories d'agents : les agents de type "serveur", qui sont identifiés par une référence fixe, et les agents de type "client", qui sont identifiés par une référence variable, que l'on peut qualifier d'éphémère, délivrée par le module de gestion de configuration, 131 ou 231a.

20 Les agents communiquent entre eux à l'aide d'entité dites "unités de donnée de protocole" ou "*pdu*" (pour "protocol data unit", selon la terminologie anglo-saxonne) constituant une référence de destination et une référence de source. On pourrait également appeler cette "*pdu*" particulière "*SmartTP pdu*", en référence au terme anglais "Smart Card" (carte à puce) couramment utilisé. Les "*pdu*" utilisent notamment les références définies ci-

25 dessus.

Une "*SmartTP pdu*", ou plus simplement "*pdu*" ci-après, comporte une référence source, une référence de destination, un ensemble de bits constituant des drapeaux ou "flags" qui précisent la nature de la "*pdu*", et des données optionnelles :

- 30 - le drapeau "*OPEN*" (ouvert) est positionné pour indiquer l'ouverture d'une session ;

19

- le drapeau "*CLOSE*" (fermé) indique la fermeture d'une session ;

et

- Le drapeau "*BLOCK*" (verrouillé) indique que l'agent est en attente d'une réponse de son correspondant et suspend toute activité.

5 On appellera jeton une "*pdu*" qui ne comporte pas de données.

L'entité "*SmartTP*" contrôle l'existence de l'agent destinataire et réalise la commutation d'un paquet vers ce dernier.

Une session agent "*S-Agent*" possède trois états remarquables, à savoir :

10 - un état déconnecté : aucune session n'est ouverte avec un autre agent

- un état connecté : une session est ouverte avec un autre agent, une session "*S-Agent*" étant identifiée par une paire de références ; et

- un état bloqué, l'agent étant connecté et attendant une réponse
15 de son correspondant.

Le mécanisme d'établissement d'une session "*S-Agent*" est le suivant :

- une nouvelle instance d'un agent client est créée (côté carte à puce ou terminal), cet agent étant identifié par une référence éphémère pseudo-unique ;
20

- l'agent client émet une "*pdu*" à destination d'un agent serveur (dont la référence est connue par ailleurs) avec le drapeau "*OPEN*" positionné et l'agent client passe à l'état connecté ou bloqué selon la valeur du drapeau "*BLOCK*" ; et

25 - l'agent serveur reçoit la "*pdu*" avec le drapeau "*OPEN*" et passe à l'état connecté

Une fois une session ouverte, deux agents échangent des données via des "*pdu*".

Le mécanisme de fermeture d'une session est le suivant :

30 - un agent émet une "*pdu*" avec le drapeau "*CLOSE*" positionné (et qui comporte éventuellement des données ; et

20

- l'autre agent reçoit une "pdu" avec le drapeau "CLOSE" positionné (et qui comporte éventuellement des données) et la session "S-Agent" passe à l'état déconnecté.

5 La figure 3 illustre de façon schématique le diagramme d'états des sessions "S-Agent", telles qu'elles viennent d'être rappelées.

Les couches 130 et 230a gèrent des tables (non représentées) qui contiennent la liste des agents présents, côté terminal hôte 1 et carte à puce 2a.

10 De façon pratique, les agents permettent d'échanger des données (de l'hypertexte, par exemple), mais également de déclencher des transactions réseau, autorisant des communications entre la carte à puce 2a et un serveur éloigné 4 (figure 2).

15 Les modules de gestion de configuration, 131 et 231a, respectivement, sont assimilables à des agents particuliers. Par exemple, le module 131, côté terminal hôte 1, gère notamment des informations relatives à la configuration de ce terminal (modes de fonctionnement), liste des autres agents présents, etc. Le module 231a, côté carte à puce 2a, a des fonctions analogues. Ces deux agents peuvent être mis en communication l'un avec l'autre pour établir une session.

20 De façon pratique, la carte à puce 2a est avantageusement "adressée" par utilisation d'une adresse "URL" (pour "Universal Resource Locator") définissant un rebouclage sur le terminal 1 lui-même, et non un pointage sur un serveur externe. A titre d'exemple, la structure de cette "URL" est habituellement la suivante :

25 [http://127.0.0.1:8080\(1\),](http://127.0.0.1:8080(1),)

dans laquelle 127.0.0.1 est l'adresse "IP" de rebouclage et 8080 est le numéro de port.

30 La figure 4 illustre de façon simplifiée l'architecture logique d'un système selon l'invention du type représenté sur la figure 2, mais décrite de façon plus détaillée. La carte à puce 2a comprend plusieurs agents, dont

21

deux seulement ont été représentés : un agent de type non précisément défini 232a₁ et un agent 232a₂, de type dit "WEB". La pile logique comprend, les couches de protocole inférieures, référencées 200a, répondant aux normes ISO 7816-3 (figure 2 : CCa₁ et CCa₂), le gestionnaire de commandes "APDU" 201a₁, et le multiplexeur de paquets 230a, ce dernier étant interfacé aux agents, notamment l'agent "WEB" 231a₂.

Du côté terminal 1, il existe deux piles, l'une communiquant avec le réseau Internet *RI*, l'autre avec la carte à puce 2a. La première pile comprend les organes 11 (figure 2 : C₁ et C₂) d'accès au réseau (normes OSI 1 et 2) et les couches de protocole "TCP/IP" (figure 2 : C₃ et C₄), référencées 100. Ces dernières couches sont interfacées avec le navigateur "WEB" 10. L'autre pile comprend les couches de protocole inférieures, référencées 101, répondant aux normes ISO 7816-3 (figure 2 : C₁ et C₂), le gestionnaire 102 d'ordres "APDU" et le multiplexeur de paquets 130, ce dernier étant interfacé avec des agents, dont un seul 132, est représenté. Ce dernier, que l'on supposera de "type réseau", peut en outre communiquer, d'une part avec le navigateur 10, via les couches "TCP/IP" 101, d'autre part avec le réseau Internet *RI*, via ces mêmes couches "TCP/IP" 101 et l'organe 11, d'accès au réseau *RI*.

Le gestionnaire d'ordres "APDU" 201a est également interfacé avec une ou plusieurs couches de niveau applications, que l'on appellera simplement applications. Ces applications, A₁, ..., A_i, ..., A_n, sont, comme il a été indiqué, des applications de type conventionnel.

En résumé, la fonction client/serveur "WEB", fournie par la carte à puce 2a, peut être réalisée par l'association de l'agent "WEB" 232a₁ dans la carte à puce et de l'agent réseau 132 dans le terminal 1, et par la mise en œuvre de sessions entre agents, comme il a été décrit.

La carte à puce 2a présente donc bien la fonctionnalité client/serveur "WEB". En outre, selon une caractéristique avantageuse du procédé de l'invention, n'importe quelle application conventionnelle, A₁ à A_n, du type

22

"CGA" précité, peut être activée au travers de ce client/serveur "WEB", soit par le navigateur "WEB" 10 présent dans le terminal 1, soit par un navigateur éloigné 4, localisé en un point quelconque du réseau Internet *RI*, par la mise en œuvre de sessions entre agents. Selon le procédé de l'invention, les applications, A_1 à A_n , ne nécessitent pas d'être ré-écrites et sont mises en œuvre telles quelles.

Dans le cadre de l'invention, tout ou partie des applications A_1 à A_n peut être constitué par des applications associées à un ou plusieurs protocole(s) "PE" et/ou un ou plusieurs protocole(s) "PL", et chargé dans une mémoire de la carte à puce 2a. Des données représentant un ou plusieurs profils "PA" peuvent également être stockées dans la carte à puce 2a.

La fonctionnalité client/serveur "WEB" offerte par la carte à puce 2a n'est pas suffisante pour qu'une application puisse s'exécuter. Il est nécessaire de lui adjoindre une fonctionnalité supplémentaire.

En effet, selon un autre aspect de l'invention, la fonction serveur "WEB" offerte par la carte à puce 2a inclut un mécanisme similaire à la fonction dite "CGI" (pour "Common Gateway Interface" ou "interface de passerelle") implantée dans les serveurs "WEB" classique.

Avant de décrire un exemple d'architecture conforme à l'invention, permettant de réaliser une fonction de ce type, au sein même de la carte à puce, il est utile de rappeler les principales caractéristiques d'un mode de fonctionnement "CGI".

Le "CGI" est une spécification de mise en œuvre, depuis un serveur "WEB", d'applications écrites pour les systèmes d'exploitation "UNIX" (marque déposée), "DOS", ou "WINDOWS" (marque déposée). A titre d'exemple, pour le système d'exploitation "UNIX", la spécification est "CGI 1.1" et pour le système d'exploitation "WINDOWS 95", la spécification est "CGI 1.3".

Toujours à titre d'exemple, une requête "HTTP" pour une adresse "URL", du type :

"http://www.host.com/cgi-bin/xxx.cgi" (2),

dans laquelle "host" se réfère à un système hôte (généralement éloigné), est interprétée par un serveur "WEB" comme l'exécution d'un script de commande, de type "CGI" nommé "xxx" et présent dans le répertoire "cgi-bin" de ce système hôte. Bien que le nom du répertoire puisse être *a priori* quelconque, par convention, c'est le nom donné au répertoire stockant les scripts de type "CGI". Un script est une suite d'instructions du système d'exploitation du système hôte dont le résultat final est transmis au navigateur "WEB" émetteur de la requête précitée. Différents langages peuvent être utilisés pour écrire ce script, par exemple le langage "PERL" (marque déposée).

De façon pratique, la requête est habituellement affichée sur un écran informatique sous la forme d'un formulaire compris dans une page "HTLM". Le langage "HTLM" permet de traduire un formulaire en une adresse "URL". Le formulaire comporte un ou plusieurs champs, obligatoires ou non, qui sont remplis par un utilisateur à l'aide des moyens de saisie habituels : clavier pour le texte, souris pour les cases à cocher ou les boutons dits "radio", etc. Le contenu du formulaire (ainsi qu'éventuellement des informations et instructions dites "cachées") est émis à destination du serveur "WEB". Le code "HTLM" de la page décrit la structure matérielle du formulaire (cadre, graphisme, couleur, et tout autre attribut), ainsi que la structure des champs de données à saisir (nom, longueur, type de données, etc.).

La transmission peut s'effectuer selon deux types de formats principaux. Un premier format utilise la méthode dite "POST" et un second la méthode dite "GET". Une information de type de format est présente dans le code de la page formulaire.

Ce mécanisme n'est cependant pas directement transposable à une carte à puce, même si celle-ci offre la fonctionnalité client/serveur "WEB" conformément à l'une des caractéristiques de l'invention.

24

On va maintenant décrire un exemple d'architecture permettant d'activer une application quelconque, de type conventionnel, via un serveur "WEB" sur la carte à puce, par référence à la figure 5.

Parmi les agents intelligents, conforme à l'un des aspects de l'invention, on prévoit des agents intelligents particuliers, que l'on appellera ci-après "Agents traducteurs de script" ou de façon abrégée "ATS". Le script est alors interprété par un des agents intelligents. Cette traduction peut être réalisée de différentes manières :

a/par l'agent "WEB" 232a₁ lui-même, qui est doté dans ce cas d'une double capacité ;

b/par un agent script unique capable de traduire l'ensemble des scripts présents dans la carte à puce 2a ;

c/par un agent de script dédié que l'on appellera "ATSD" ci-après (un agent par script) ; ou

d/par un agent "APDU" 2010a du gestionnaire d'ordres "APDU" 201a, qui est doté, dans ce cas, d'une double capacité.

L'agent "APDU" 2010a est une composante de la couche gestionnaire d'ordres "APDU" 201a. Cette dernière est une couche capable de centraliser tous les ordres "APDU" émis et/ou reçus par le système, de sélectionner des applications, parmi A_1 à A_n , mais également d'offrir une interface de type agent intelligent. Elle est donc capable, selon l'une des caractéristiques de l'invention de communiquer avec tous les agents intelligents (via des sessions), que ces agents soient localisés dans le terminal 1 ou la carte à puce 2a.

Dans le cas c/ ci-dessus, une session est ouverte entre l'agent "WEB" 232a₁ et l'un des agents "ATSD".

La figure 5 illustre un exemple d'architecture pour laquelle les agents traducteurs sont du type "ATSD". Ils sont référencés ATS_1 à ATS_n et associés aux applications A_1 à A_n . L'application sélectionnée étant supposée

25

être l'application A_i , la session s'établit entre l'agent "WEB" 232a₁ et l'agent ATS_i .

Un agent traducteur de script génère une suite d'ordres "APDU". Une session est ouverte entre l'agent traducteur, par exemple l'agent ATS_i , et l'agent "APDU" 2101a. Les ordres sont alors émis vers l'agent "APDU" 2101a. Le gestionnaire d'ordres "APDU" 210a sélectionne l'application "CGA" A_i et lui transmet les ordres "APDU", ordres traduits et donc conventionnels, qu'elle est en mesure de comprendre. Cette application est donc correctement activée, sans avoir à la modifier ou à la réécrire.

Les réponses de l'application A_i sont transmises au gestionnaire d'ordres "APDU" 210a, à l'agent "APDU" 2010a, puis de nouveau à l'agent ATS_i (et de façon plus générale à l'agent traducteur de script).

Les différents cheminements sont représentés symboliquement sur la figure 5 par des traits pleins reliant les blocs fonctionnels, ou en pointillés à l'intérieur de ces blocs.

Le procédé selon l'invention utilise les deux caractéristiques qui viennent d'être rappelées : fonctionnement de la carte à puce en tant que serveur/client "WEB", incluant une fonction "CGI".

On va maintenant décrire de façon détaillée les différentes phases et étapes du procédé selon l'invention par référence aux figures 6A à 8.

La première phase concerne l'enregistrement d'un profil d'abonné dans un serveur d'annuaire particulier que l'on référencera SA_i ci-après.

Dans une première étape, illustrée par la figure 6A, la carte à puce 2a est adressée par le navigateur 10 du terminal 1, via les couches 13 et 23a. On récupère, par une commande de type "GET" par exemple, un formulaire de chargement à partir de la carte à puce 2a, formulaire en langage "HTML" que l'on appellera arbitrairement "download.html".

Cette récupération est effectuée en consultant une page correspondante dont l'URL est typiquement de la forme suivante :

26

`http://127.0.0.1:8080/download.html`

(3),

dans laquelle `http://127.0.0.1:8080` est l'adresse URL de rebouclage proprement dite, telle qu'elle a été définie par la relation (1), et "download.html" la page "HTML" à obtenir. Cette requête met en œuvre une
5 session entre agents intelligents comme il a été décrit en regard des figures 2 à 4, selon un premier aspect de l'invention. La carte à puce 2a joue alors le rôle d'un serveur "WEB".

La carte à puce 2a envoie le formulaire "download.html" lors d'une deuxième étape, toujours par ouvertures de sessions entre agents
10 intelligents appariés, selon le procédé de l'invention. Le formulaire obtenu peut être affiché sur un écran 5 par l'intermédiaire du navigateur 10 et est référencé *P* sur la figure 6A qui illustre schématiquement ce processus. Ce formulaire constitue une page d'accueil pour l'internaute désirant s'enregistrer sur un serveur d'annuaire. La carte à puce se comporte alors
15 comme un serveur "WEB".

La page *P* peut comporter, de façon usuelle, différents éléments de type graphique ou de type texte, ainsi que des éléments interactifs de commande (bouton de type dit "radio", cases à cocher, zones d'entrées de données, etc.).

20 On va supposer, dans un premier temps que la carte à puce 2a n'offre, à son porteur (non représenté), que la possibilité de s'enregistrer sur un serveur d'annuaire unique, référencé SA_u , et selon un profil unique d'abonné, référencé PA_u . On suppose également que ce profil unique PA_u est enregistré dans la carte à puce 2a. Dans cette hypothèse, le formulaire *P*
25 (c'est-à-dire la page d'accueil) affiché sur l'écran 5, peut se réduire à une présentation minimale, dont la figure 6B illustre un exemple possible : formulaire P_1 .

Le formulaire P_1 comprend diverses zones de textes, sous la référence unique Z_i . Ces zones affichent typiquement le nom "xxx" du
30 serveur d'annuaire (SA_u), l'action proposée "*enregistrement*" et diverses aides (par exemple "*cliquer ici*"). Puisque l'on a supposé que les données du

27

profil d'abonné PA_u étaient enregistrées dans la carte à puce 2a, il suffit de prévoir un bouton d'envoi B_s . Le fait pour l'internaute de cliquer sur ce bouton à l'aide d'une souris (figure 1A : 6b) ou d'appuyer sur la touche "entrée" d'un clavier (figure 1A : 6a), déclenche l'envoi du formulaire vers la

5 carte à puce 2a.

Dans une autre variante du procédé selon l'invention, les données afférentes au profil de l'abonné sont saisies directement par celui-ci. Dans cette hypothèse, le formulaire est plus complexe. La figure 6C illustre un exemple possible de formulaire, référencé P_2 . Il comprend une première

10 zone de texte fixe Z_{11} , similaire à celle de la figure 6B (Z_1) et une ou plusieurs zone(s) de saisie de données, sous la référence unique Z_{12} . On prévoit comme précédemment un bouton d'envoi B_s , mais aussi avantageusement un bouton B_{raz} de ré-initialisation du formulaire P_2 , qui permet d'effacer les données saisies en cas d'erreur. La ou les zones de saisies de données Z_{12}

15 peu(ven)t être du type dit "TEXTAREA" en langage "HTML" et présenter une facilité dite d' "ascenseur" pour l'affichage déroulant de textes longs

Le code "HTML" nécessaire pour programmer un tel formulaire est bien connu en soi et est à la portée de l'homme de métier. Il n'est pas nécessaire de le détailler de nouveau. On peut cependant indiquer qu'il

20 contient notamment une ligne de code en langage "HTML" qui se présente typiquement sous la forme :

$$\langle \text{form action} = \text{"http://127.0.01:8080/cgi-smart/pe"} \rangle \quad (4)$$

dans laquelle $\text{http://127.0.01:8080}$ est l'URL de rebouclage de la relation (1), cgi-smart le répertoire "CGI" précité contenant un script "pe" associé à une

25 des applications stockées dans la carte à puce 2a, référencée par exemple A_e . cette application permet l'enregistrement de l'abonné (internaute) sur l'annuaire SA_u avec le profil PA_u . Cette action s'effectue de la manière décrite en regard de la figure 5, par mise en œuvre des fonctionnalités "CGI", d'une part, et client/serveur, d'autre part, offertes par la carte à puce 2a.

30 L'application A_e se comporte comme un client.

28

Dans le premier cas (figure 6B), il n'est pas nécessaire de passer des paramètres à la carte à puce 2a. En effet, les données de profil d'abonné PA_u sont uniques et enregistrées dans la carte à puce 2a.

5 Dans le second cas (figure 6C), les données saisies sont passées en tant que paramètres à la carte à puce 2a, sous la forme d'une requête "HTTP".

La figure 6D illustre schématiquement le processus global de la phase d'enregistrement d'un internaute sur un serveur d'annuaire SA_u , constitué par un des serveurs 4 (figures 2 ou 4).

10 La référence unique S_{WEB} regroupe différents modules de la figure 5 permettant à la carte à puce 2a d'offrir les fonctionnalités combinées de client/serveur WEB et de passerelle "CGI". On a également supposé que l'application A_e permettant la mise en œuvre du protocole d'enregistrement "PE" était associée à un agent traducteur de script dédié At_e ; il s'agit d'une
15 configuration conforme à celle illustrée par la figure 5. Cependant, comme il a été indiqué, la traduction des scripts peut s'effectuer d'autres manières (par l'agent "WEB" 232a, (figure 5), etc. L'envoi du formulaire, par ouverture de sessions entre agents intelligents, va permettre d'activer l'application A_e , par l'intermédiaire de l'agent traducteur de script At_e .

20 Lors d'une étape ultérieure, l'application A_e pose une requête "HTTP" par ouverture de sessions entre paires d'agents intelligents, notamment impliquant un agent de type "réseau" (figure 5 : 132). La requête est transmise au serveur d'annuaire SA_u , avec passage de paramètres. Les paramètres sont constitués notamment par les données de profil abonné
25 PA_u , de façon à permettre son enregistrement dans l'annuaire. L'adresse "URL" du serveur d'annuaire est obtenue à partir du profil d'abonné SA_u enregistré dans la carte à puce 2a ou à partir des données saisies dans le formulaire P_2 .

A priori, le processus d'enregistrement est terminé à ce stade. Il peut
30 cependant comprendre une ou plusieurs étapes supplémentaires. Une de ces étapes peut consister en l'envoi par l'annuaire d'un accusé de réception,

sous forme d'une requête "HTTP" adressant la carte à puce 2a. L'accusé de réception peut comprendre une information indiquant que l'inscription s'est déroulée de façon satisfaisante, ou au contraire un code d'erreur. Dans ce dernier cas, le processus d'enregistrement doit être répété. Le serveur peut
5 requérir l'envoi de données manquantes ou la ré-émission de données incorrectes ou corrompues. La demande d'enregistrement peut également être rejetée, notamment si la limite de validité de l'abonnement est dépassée.

Dans une variante préférée du procédé selon l'invention, il est
10 possible, pour un internaute de s'enregistrer sur plusieurs annuaires différents. Dans cette variante de réalisation, il est en général nécessaire de disposer également de plusieurs protocoles d'enregistrement. Pour ce faire, plusieurs applications associées à ces protocoles sont stockées dans la carte à puce 2a, que l'on peut référencer $A_{e1}, \dots, A_{ei}, \dots, A_{en}$, en admettant que
15 le nombre maximum de protocoles distincts est n .

Comme précédemment, les données associées aux profils d'abonné, que l'on référencera $PA_1, \dots, PA_i, \dots, PA_q$, peuvent être stockées dans la carte à puce 2a, ou au contraire fournis, au coup par coup, par l'internaute selon une méthode similaire à ce qui a été décrit en regard de la
20 figure 6C, par saisie dans un formulaire approprié. q est le nombre maximum de profils d'abonné disponibles. On notera que q n'est pas forcément égal à n . En effet, un serveur d'annuaire donné, que l'on référencera arbitrairement SA_i , peut accepter plusieurs occurrences distinctes d'un même abonné (internaute), d'une part. D'autre part, plusieurs serveurs d'abonné, bien que
25 distincts, peuvent accepter un même profil d'abonné et éventuellement partager un protocole d'enregistrement commun.

Pour fixer les idées, on va supposer que la carte à puce 2a stocke quatre profils d'abonnés distincts, PA_A à PA_D , chacun des profils permettant de s'enregistrer sur un seul serveur d'annuaire, soit SA_A à SA_D . Un
30 formulaire, ou page d'accueil, référencé P_3 , permettant cet enregistrement, peut se présenter comme illustré schématiquement par la figure 6E. il

30

comprend une première zone de texte d'en-tête Z_{ie} similaire à la zone de texte Z_i de la figure 6B, éventuellement complétée par des zones graphiques. Il comprend quatre zones de textes supplémentaires, Z_{ia} à Z_{id} , associée aux quatre serveurs d'annuaires, SA_A à SA_D . Le formulaire permet
 5 de sélectionner un ou plusieurs, voire tous.

Pour effectuer un choix entre ces serveurs d'annuaires, on peut prévoir des zones dites "cases à cocher", CC_A à CC_D . A titre d'alternative, on peut prévoir des hyperliens sur la page d'accueil P_3 , chaque hyperlien adressant la carte à puce 2a par l'intermédiaire d'une dresse de rebouclage
 10 du type de celle de la relation (1), mais avec des paramètres distincts.

Comme dans le cas de la figure 6B, on prévoit un bouton d'envoi B_S , permettant de transmettre le contenu du formulaire à la carte à puce 2a.

Quelle que soit la méthode utilisée pour effectuer la sélection de tout ou partie des serveurs d'annuaires, les paramètres passés à la carte à puce 2a doivent permettre de sélectionner un ou plusieurs profils d'abonné,
 15 PA_A à PA_D , et en dériver une ou plusieurs adresses "URL". Les actions demandées, par les paramètres passés à la carte à puce 2a, sont typiquement du type :

$$?sa_i=enr+pa_i \quad (5),$$

20 avec " sa_i " le nom du serveur d'annuaire d'indice arbitraire i parmi les n possibles, " enr " l'action requise d'enregistrement proprement dit et " pa_i " le profil d'abonné à utiliser parmi les q possibles.

Une ou plusieurs requêtes "HTTP" sont posées et transmises aux serveurs d'annuaires concernés, SA_A à SA_D (figure 6E) et dans le cas
 25 général SA_A à SA_n , s'il existe n serveurs d'annuaire sélectionnables.

Le choix présenté sur la page d'accueil P_3 est naturellement fonction de la carte à puce 2a insérée dans le lecteur 3. Les choix présentés dépendent des droits qui sont accordés à l'internaute possesseur de la carte à puce 2a, notamment des abonnements souscrits à des services donnés et
 30 de leurs périodes de validité.

Une deuxième phase du procédé selon l'invention, c'est-à-dire la localisation, sur le réseau Internet, d'un internaute associé à un identifiant quelconque peut se dérouler de façon très similaire à la phase d'enregistrement.

5 Pour ce faire, il est nécessaire d'interroger un ou plusieurs serveur(s)
d'annuaire(s). Il est nécessaire aussi de disposer d'au moins un protocole
"PL" spécifique de localisation de cet internaute. Enfin, s'il existe plusieurs
serveurs d'annuaires interrogeables, SA_1 à SA_n , il est généralement
nécessaire également, comme dans le cas de l'enregistrement, de disposer
10 de plusieurs protocoles de localisation distincts.

Ces protocoles de localisation peuvent être mis en œuvre à l'aide d'applications stockées dans la carte à puce 2a.

Le processus de localisation se déroule de façon tout à fait similaire à celui de l'enregistrement de l'internaute sur un ou plusieurs serveurs d'annuaire SA_i . La seule exception notable est qu'un profil d'abonné PA_j n'est plus explicitement requis. Il suffit de fournir à la carte à puce 2a l'identifiant de l'internaute recherché et l'adresse du serveur d'annuaire SA_i , ou pour le moins des paramètres permettant à l'application associée à l'un des protocoles de localisation de déterminer cette adresse "URL". Un profil d'abonné PA_j peut toutefois être utilisé pour en dériver automatiquement l'adresse "URL" du serveur d'annuaire SA_i à l'aide duquel lequel un internaute désire localiser un autre internaute. Comme il a été indiqué, l'identifiant de l'internaute recherché peut être son adresse e-mel, adresse qui se présente typiquement sous la forme suivante :

25 pseudo@fournisseur.com (6),

avec "pseudo" le nom d'utilisateur de messagerie de l'internaute ou plus généralement un pseudonyme, et "fournisseur.com" le nom et le suffixe du prestataire de service Internet",.com" pouvant être remplacé selon les cas par divers suffixes : ".fr", ".net", etc.).

La figure 7 illustre les principales étapes de la phase de localisation d'un internaute par interrogation d'un annuaire SA_i.

32

Dans une première étape la carte à puce 2a est adressée par le navigateur 10 du terminal 1, via les couches 13 et 23a. On récupère, par une commande de type "GET" par exemple, un formulaire de chargement à partir de la carte à puce 2a sous la forme d'une page d'accueil référencée P . Cette

5 page d'accueil peut prendre différents aspects, similaires notamment à ceux décrits en regard des figures 6C ou 6E. Selon qu'il y ait un choix ou plusieurs choix possibles, l'internaute sélectionne un ou plusieurs serveurs d'annuaires et fournit des données d'identification de l'internaute recherché. Sur la figure 7, on a supposé qu'un seul serveur d'annuaire SA_i était interrogeable.

10 La page est transmise sous forme d'une requête "HTTP" à la carte à puce 2a et est interprétée par un agent traducteur de script At_i associé à une application A_i de mise en œuvre de protocole "PL".

Par le double mécanisme client/serveur "WEB" et "CGI" (module référencé S_{WEB} comme précédemment), une requête du type :

15 $\text{http://127.0.0.1/? sa}_i=\text{loc+pseudo@fournisseur.com}$ (7),
est interprétée par la carte à puce 2a comme une demande de localisation de l'internaute dont l'identifiant est (6) sur le serveur d'annuaire sa_i .

Une requête "HTTP" est transmise à ce serveur qui renvoie les informations demandées, dans la mesure où elles sont disponibles. Il

20 recherche dans sa base de données une adresse "IP" correspondant aux données d'identification reçues. En cas de succès, c'est-à-dire si l'internaute demandeur est effectivement enregistré, si cet internaute a le droit d'obtenir cette adresse et si les données reçues sont correctes, les données retransmises comprennent l'adresse "IP" de l'internaute recherché, ce qui

25 permet de le localiser.

Ces différentes étapes mettent en œuvre des sessions entre agents appariés, selon un des aspects de l'invention.

On peut également stocker dans la carte à puce 2a plusieurs applications, chacune étant destinée à la mise en œuvre d'un protocole de

30 localisation distinct, a priori associé à un serveur d'annuaire également distinct.

Dans une variante préférée du procédé selon l'invention, on stocke dans la carte à puce 2a des applications permettant la mise en œuvre de plusieurs protocoles d'enregistrement, plusieurs protocoles de localisation et des fichiers de données pour l'enregistrement de plusieurs profils d'abonné.

5 Cette disposition avantageuse permet de transformer la carte à puce 2a en base de données portable multi-annuaire comme illustré schématiquement par la figure 8. Sur cette figure, le terminal 1 n'a pas été représenté. Il est cependant clair que celui-ci est nécessaire à la mise en œuvre du procédé selon l'invention.

10 Les protocoles d'enregistrement, les protocoles de localisation et les profils d'abonné portent les références uniques, PE_x , PL_y et PA_z , respectivement, avec x le nombre de protocoles d'enregistrement, y le nombre de protocoles de localisation et z le nombre de profils d'abonnés distincts. Cet ensemble permet d'établir des connexions avec n serveurs
15 d'annuaires distincts, soit pour y enregistrer un internaute porteur de la carte à puce 2a, soit pour localiser un internaute sur le réseau Internet RI .

Dans une autre variante encore du procédé selon l'invention, l'utilisation d'une carte à puce 2a permet une authentification robuste de son possesseur, lors de la phase d'enregistrement et/ou de la phase de
20 localisation. En effet, il est possible de stocker des données de sécurité dans la carte à puce 2a qui reste propriété de son possesseur. De telles données de sécurité peuvent être constituées par des clés de chiffrement.

Du fait que, selon l'un des aspects avantageux du procédé selon l'invention, la carte à puce peut communiquer directement avec le réseau
25 Internet, par la mise en œuvre de sessions entre agents intelligents, ces données n'ont pas à être transmises à un dispositif externe, serait ce le terminal 1. Les traitements touchant à la sécurité sont effectués directement par la carte à puce 2a. Cette façon de procéder offre donc un degré de sécurité beaucoup plus élevé que la simple utilisation de couches logicielles
30 dites sécurisées des navigateurs "WEB" récents, connues sous l'abréviation anglo-saxonne "SSL" (pour "Secure Socket Layer").

L'authentification proprement dite peut s'effectuer en ayant recours à la technique dite de certificat, en association avec les clés de chiffrement précitées stockées dans la carte à puce. Cette procédure peut nécessiter des transactions supplémentaires entre la carte à puce 2a et le ou les 5 serveur(s) d'annuaire concerné(s), à l'aide de requêtes "HTTP" transitant par le réseau Internet RI. En fonction du résultat, positif ou négatif, de l'authentification, l'internaute est autorisé ou non à effectuer les traitements, enregistrements ou localisations qu'il désire réaliser.

A la lecture de ce qui précède, on constate aisément que le procédé 10 de l'invention atteint bien les buts qu'elle s'est fixés.

Il permet notamment à un internaute de s'enregistrer sur un ou plusieurs serveurs d'annuaires et/ou de localiser un internaute sur le réseau Internet, également par l'intermédiaire de un ou plusieurs annuaires. La carte à puce présentant les fonctionnalités combinées d'un client/serveur "WEB" et 15 d'une passerelle "CGI", cette disposition permet des communications directes entre la carte à puce et le ou les serveurs d'annuaire. Elle autorise de ce fait le stockage des logiciels spécifiques nécessaires à la mise en œuvre des protocoles d'enregistrement et/ou de localisation, ce qui permet une grande mobilité. Un ou plusieurs profils d'abonné peuvent également 20 être stockés dans la carte à puce. L'internaute n'est plus astreint à l'utilisation de terminaux configurés spécifiquement pour les protocoles précités.

En particulier, dans une variante de réalisation préférée, la carte à puce est transformée en base de données portable multi-annuaire.

25 Le procédé selon l'invention est tout à fait compatible avec l'existant. Il n'est pas requis que l'internaute recherché se soit enregistré sur un ou plusieurs serveurs d'annuaires en faisant usage du procédé selon l'invention. Les transmissions sur le réseau Internet s'effectuent selon les protocoles en vigueur et les communications entre le terminal et la carte à puce font appel 30 au protocole normalisé "ISO" précité. On peut donc mettre en œuvre un lecteur de carte à puce standard. Seule la présence d'une couche logicielle

35

spécifique dans le terminal est nécessaire, ce qui ne nécessite que peu de modifications et peut être réalisé une fois pour toute, quel que soit le nombre de protocoles d'enregistrement, de localisation et/ou de profils d'abonné portés par la carte à puce, et quelle que soient leurs natures.

- 5 Enfin, l'utilisation d'une carte à puce permet une sécurisation des transactions et, notamment, une authentification "robuste".

Il doit être clair cependant que l'invention n'est pas limitée aux seuls exemples de réalisations explicitement décrits, notamment en relation avec les figures 2 à 8.

- 10 En particulier, il n'est pas nécessaire que les deux séries de logiciels propriétaires, "PE" et "PL" soient stockées dans la carte à puce, bien que cette disposition soit particulièrement avantageuse. A titre d'exemple non limitatif, la (les) phase(s) d'enregistrement, dans un ou plusieurs serveurs d'annuaire(s), pouvant être réalisée(s) une fois pour toute, ou pour le moins
- 15 étant *a priori* moins fréquente(s) que les phases de localisation, on pourrait se contenter de ne stocker dans la carte à puce que les applications spécifiques associées à cette dernière opération. De même, comme il a été indiqué, il est possible de ne pas enregistrer dans la carte à puce les profils d'abonné "PA" (les données pouvant être fournies en temps réel au moment
- 20 de l'enregistrement de l'abonné dans un serveur d'annuaire particulier). Il est encore possible de n'enregistrer qu'une partie des profils d'abonné, profils qui pourront être fournis de façon automatique.

- L'invention concerne aussi un procédé de mise en relation d'un premier usager avec au moins un serveur d'annuaire, en vue de son enregistrement
- 25 et/ou de la localisation d'au moins un deuxième usager sur un réseau notamment de type Internet, ladite mise en relation s'effectuant par l'intermédiaire d'un terminal muni d'un lecteur de carte à puce et d'au moins une pièce de logiciel dite d'enregistrement et/ou de localisation, le terminal et la carte à puce comprenant des moyens de traitement d'information et des
- 30 moyens de stockage d'information, ledit terminal étant connecté à chacun desdits serveurs d'annuaire via ledit réseau de type Internet et

36

communiquant avec ladite carte à puce selon un premier protocole déterminé, caractérisé en ce qu'au moins l'une desdites pièces de logiciel (A_e , A_i) est stockée dans ladite carte à puce (2a) ; en ce que cette carte à puce (2a) comprenant une première pièce de logiciel (23a), formant une

5 couche protocolaire de communication spécifique, et ledit terminal (1) comprenant une seconde pièce de logiciel (13), formant une couche protocolaire de communication spécifique, lesdites première et seconde pièces de logiciel (13, 23a) comprennent en outre au moins une paire de premières entités logicielles appariées (132, 232a), chacune desdites entités

10 (132, 232a) coopérant l'une avec l'autre, grâce auxdits moyens de traitement d'information, de manière à permettre l'établissement d'une session d'échanges de données bidirectionnels entre au moins ledit terminal (1) et ladite carte à puce (2a), et/ou ledit réseau de type Internet, de manière à ce que ladite carte à puce (2a) offre la fonctionnalité d'un client/serveur "WEB" ;

15 en ce que ladite carte à puce (2a) comprend, dans les moyens de stockage d'information, au moins une deuxième entité logicielle (AT_e , AT_i) coopérant avec ladite seconde pièce de logiciel spécifique (23a) pour que ladite carte à puce offre une fonctionnalité d'interface passerelle dite "CGI" :

et en ce qu'il comprend au moins les étapes suivantes :

- 20 1/ ouverture d'une première séquence d'échanges de données entre au moins ledit terminal (1) et ladite carte à puce (2a) grâce auxdits moyens de traitement d'information du terminal et de la carte à puce, pour la transmission d'une requête pour que ledit navigateur de type "WEB" récupère des données permettant de sélectionner et d'activer une
- 25 desdites pièces de logiciel propriétaire (A_e , A_i), en vue de la sélection d'un desdits serveurs d'annuaire (SA_i) ;
- 2/ ouverture d'une deuxième séquence d'échanges de données entre ladite carte à puce (2a) et ledit terminal (1) pour lui transmettre lesdites données, grâce auxdits moyens de traitement d'information du terminal
- 30 et de la carte à puce ;

37

- 3/ ouverture d'une troisième séquence d'échanges de données entre ledit terminal (1) et ladite carte à puce (2a) grâce auxdits moyens de traitement d'information du terminal et de la carte à puce, pour transmettre des données de sélection et des paramètres optionnels, lesdites données et lesdits paramètres optionnels comportant une référence à une desdites pièces de logiciel d'enregistrement et/ou de localisation ;
- 4/ mise en œuvre de ladite fonctionnalité "CGI" et exécution de ladite pièce de logiciel d'enregistrement et/ou de localisation (A_e , A_l), grâce auxdits moyens de traitement d'information de la carte à puce ; et
- 5/ en résultat de ladite exécution, ouverture), grâce auxdits moyens de traitement d'information de la carte à puce, d'une quatrième séquence d'échanges de données entre ladite carte à puce (2a) et un desdits serveurs d'annuaire (SA_i), sélectionné par lesdites données de sélection, de manière à transmettre une requête pour la réalisation d'une opération déterminée d'enregistrement ou de localisation.

L'invention concerne aussi une carte à puce comprenant des moyens de traitement d'information et des moyens de stockage d'information et destinée à coopérer avec un terminal muni d'un lecteur de carte à puce, pour la mise en relation d'un premier usager avec au moins un serveur d'annuaire, en vue de son enregistrement et/ou de la localisation d'au moins un deuxième usager sur un réseau notamment de type Internet, à l'aide de protocoles d'enregistrement et/ou de localisation déterminés, caractérisé en ce que ladite carte à puce (2a) stocke, dans les moyens de stockage d'information, au moins une pièce de logiciel (A_e , A_l) associée aux dits protocoles déterminés d'enregistrement et de localisation, en ce que cette carte à puce (2a)) comporte, dans les moyens de stockage d'information, une pièce de logiciel (23a), formant une couche protocolaire de communication spécifique, comprenant en outre au moins une première entité logicielle autonome (S_i), de type dit

38

- client et une deuxième entité logicielle autonome (S_2), de type dit serveur, lesdites entités (S_2 , S_2) coopérant, grâce aux moyens de traitement d'information, de manière à ce que ladite carte à puce (2a) offre la fonctionnalité d'un client/serveur de type "WEB" et à permettre ladite mise
- 5 en relation d'un premier usager avec au moins un serveur d'annuaire (SA_i), via ledit réseau de type Internet (RI), et en ce que ladite carte à puce (2a) comprend, dans les moyens de stockage d'information, au moins une deuxième entité logicielle (AT_e , AT_i) coopérant, grâce aux moyens de traitement d'information, avec ladite pièce de logiciel
- 10 spécifique (23a), pour que ladite carte à puce (2a) offre une fonctionnalité d'interface passerelle dite "CGI" permettant l'exécution desdites pièces de logiciel (A_e , A_i) associées aux dits protocoles déterminés d'enregistrement et de localisation.

REVENDICATIONS

1. Procédé de mise en relation d'un premier usager avec au moins un serveur d'annuaire, en vue de son enregistrement et/ou de la localisation d'au moins un deuxième usager sur un réseau notamment de type Internet, ladite mise en relation s'effectuant par l'intermédiaire d'un terminal muni d'un
- 5 lecteur de carte à puce et d'au moins une pièce de logiciel dite d'enregistrement et/ou de localisation, ledit terminal étant connecté à chacun desdits serveurs d'annuaire via ledit réseau de type Internet et communiquant avec ladite carte à puce selon un premier protocole déterminé, caractérisé en ce qu'au moins l'une desdites pièces de logiciel
- 10 (A_e, A_l) est stockée dans ladite carte à puce (2a) ; en ce que cette carte à puce (2a) comprenant une première pièce de logiciel (23a), formant une couche protocolaire de communication spécifique, et ledit terminal (1) comprenant une seconde pièce de logiciel (13), formant une couche protocolaire de communication spécifique, lesdites première et seconde
- 15 pièces de logiciel (13, 23a) comprennent en outre au moins une paire de premières entités logicielles appariées (132, 232a), chacune desdites entités (132, 232a) coopérant l'une avec l'autre de manière à permettre l'établissement d'une session d'échanges de données bidirectionnels entre au moins ledit terminal (1) et ladite carte à puce (2a), et/ou ledit réseau de
- 20 type Internet, de manière à ce que ladite carte à puce (2a) offre la fonctionnalité d'un client/serveur "WEB" ; en ce que ladite carte à puce (2a) comprend au moins une deuxième entité logicielle (AT_e, AT_l) coopérant avec ladite seconde pièce de logiciel spécifique (23a) pour que ladite carte à puce offre une fonctionnalité d'interface passerelle dite "CGI" :
- 25 et en ce qu'il comprend au moins les étapes suivantes :
- 1/ ouverture d'une première séquence d'échanges de données entre au moins ledit terminal (1) et ladite carte à puce (2a), pour la transmission

40

d'une requête pour que ledit navigateur de type "WEB" récupère des données permettant de sélectionner et d'activer une desdites pièces de logiciel propriétaire (A_e, A_i), en vue de la sélection d'un desdits serveurs d'annuaire (SA_i) ;

5 2/ ouverture d'une deuxième séquence d'échanges de données entre ladite carte à puce (2a) et ledit terminal (1) pour lui transmettre lesdites données ;

10 3/ ouverture d'une troisième séquence d'échanges de données entre ledit terminal (1) et ladite carte à puce (2a) pour transmettre des données de sélection et des paramètres optionnels, lesdites données et lesdits paramètres optionnels comportant une référence à une desdites pièces de logiciel d'enregistrement et/ou de localisation ;

4/ mise en œuvre de ladite fonctionnalité "CGI" et exécution de ladite pièce de logiciel d'enregistrement et/ou de localisation (A_e, A_i) ; et

15 5/ en résultat de ladite exécution, ouverture d'une quatrième séquence d'échanges de données entre ladite carte à puce (2a) et un desdits serveurs d'annuaire (SA_i), sélectionné par lesdites données de sélection, de manière à transmettre une requête pour la réalisation d'une opération déterminée d'enregistrement ou de localisation.

20 2. Procédé selon la revendication 1, caractérisé en ce que ledit lecteur de carte à puce (3) et ladite carte à puce (2a) comprennent des première et deuxième piles protocolaires pour lesdites transmissions de données selon ledit premier protocole déterminé, définies par la norme ISO 7816, chacune comprenant au moins des couches protocolaires de
25 communication logicielles (101, 200a), dites basses, de manière à permettre lesdits échanges de données entre ladite carte à puce (2a) et ledit terminal (1), ces couches formant interface avec lesdites première (13) et seconde (23a) pièces de logiciel spécifique formant lesdites couches protocolaires de communication spécifiques, respectivement, et
30 en ce que ces pièces de logiciel (13, 23a) comprennent chacune deux

41

entités supplémentaires constituées d'un module de transfert de données (130, 230a), formant interface avec lesdites couches basses (101, 200a) des première et deuxième piles protocolaires, et d'un module de gestion (131, 231a), et en ce que lesdites premières entités de chaque paire sont
5 constituées de modules logiciels, dits agents intelligents (132, 232a1) établissant lesdites sessions.

3. Procédé selon la revendication 2, caractérisé en ce que ladite suite d'instructions à interpréter associée à chacune desdites pièces de logiciel propriétaire est constituée par un script et en ce que ladite deuxième
10 entité logicielle est constituée par un module logiciel dit agent intelligent traducteur de script (AT_e , AT_l) fournissant des ordres compréhensibles par pièces de logiciel propriétaire (A_e , A_l).

4. Procédé selon la revendication 1, caractérisé en ce que ladite étape 1/ comprend l'émission d'une requête de type dit "HTTP" selon un protocole
15 de type Internet par adressage d'une page déterminée (P_1 - P_3) en langage "HTML" contenant lesdites données de sélection et des paramètres optionnels, ladite adresse étant une adresse de type "URL" de rebouclage sur ladite carte à puce (2a).

5. Procédé selon la revendication 1, caractérisé en ce que ladite étape 2/
20 comprend l'envoi par ladite carte à puce (2a) d'un formulaire en langage "HTML" (P_1 - P_3) et en ce que ledit formulaire comprend au moins une adresse de type dit "URL" de rebouclage sur ladite carte à puce (2a) et un chemin menant à un répertoire déterminé associé à l'une desdites pièces de logiciel d'enregistrement et/ou de localisation (A_e , A_l), à lui transmettre
25 lesdits paramètres optionnels et à occasionner son exécution.

6. Procédé selon la revendication 5, caractérisé en ce que ladite étape 3/ comprend l'envoi d'une requête de type dit "HTTP" à ladite adresse "URL", désignant ledit répertoire contenant ladite pièce de logiciel

d'enregistrement et/ou de localisation (A_e , A_i), ladite requête comprenant lesdites données de sélection et lesdits paramètres optionnels.

7. Procédé selon la revendication 6, caractérisé en ce qu'une pièce de logiciel dite d'enregistrement (A_e) est associée à un premier protocole (PE_x) permettant l'enregistrement dudit usager sur un serveur d'annuaire déterminé (SA_i), en ce que lesdits paramètres optionnels sont constitués par des données définissant un profil dit d'abonné (PA_z), comprenant au moins des données dites d'identification dudit premier usager, et en ce que ladite requête "HTTP" de ladite étape 3/ comprend des premières données indiquant que l'opération demandée est ledit enregistrement et des deuxièmes données permettant d'élaborer, par ladite pièce de logiciel d'enregistrement (A_e), une adresse de type "URL" caractéristique dudit serveur d'annuaire déterminé (SA_i), et en ce que des données associées au dit profil d'abonné sont transmises, pendant ladite étape 4/, à ce serveur d'annuaire (SA_i), de manière à réaliser ledit enregistrement dudit premier usager, ledit enregistrement comprenant la détermination d'une adresse de type "IP" par association de ladite adresse de serveur d'annuaire (SA_i) et desdites données d'identification dudit premier usager.
8. Procédé selon la revendication 7, caractérisé en ce qu'il comprend au moins une étape supplémentaire consistant à l'envoi à ladite carte à puce (2a) d'un acquittement ou d'un code d'erreur.
9. Procédé selon la revendication 8, caractérisé en ce qu'il comprend des étapes supplémentaires consistant en des échanges de données entre un desdits serveurs d'annuaire (SA_i) et ladite carte à puce (2a), de manière à authentifier celle-ci ou ledit premier usager, et en ce que ladite authentification met en oeuvre un certificat et au moins une clé de chiffrement stockée dans ladite carte à puce (2a).

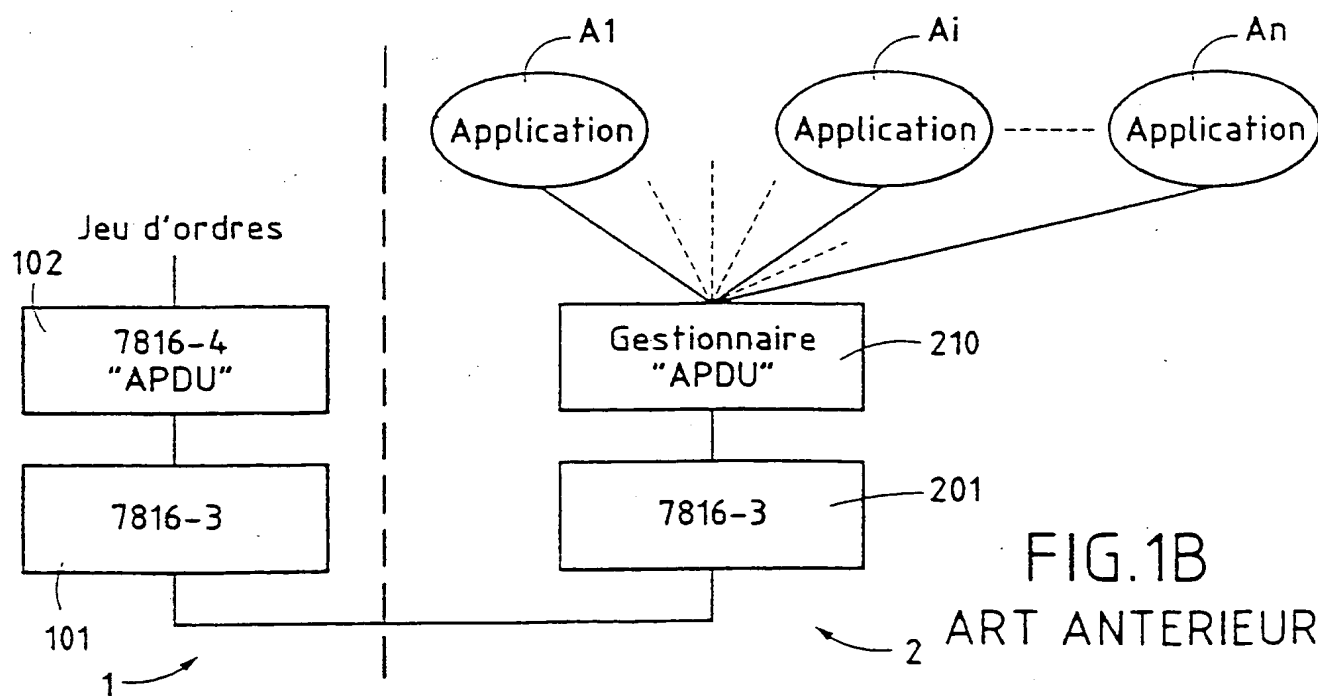
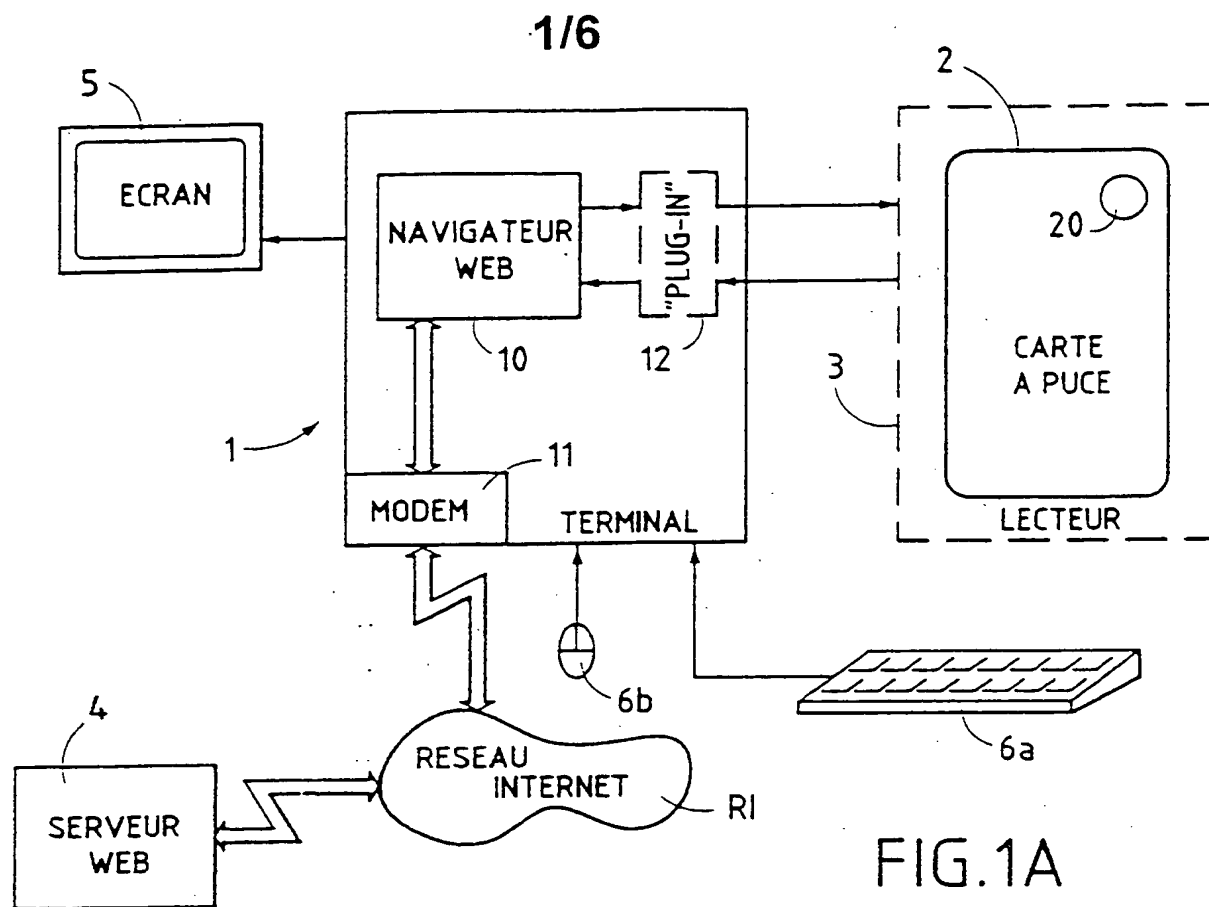
43

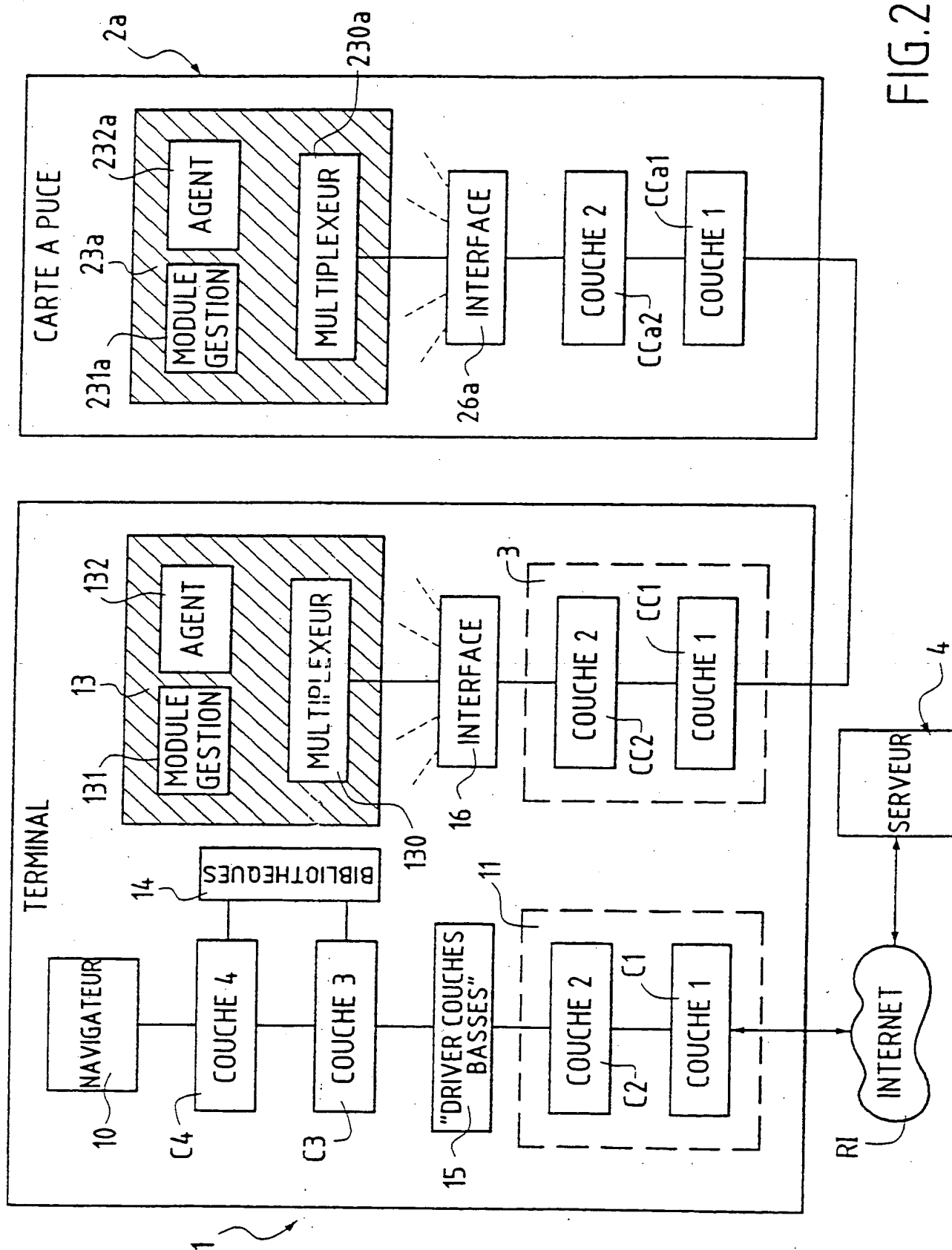
10. Procédé selon la revendication 6, caractérisé en ce qu'une pièce de logiciel dite de localisation (A_i) est associée à un second protocole (PL_j) permettant la localisation d'au moins un deuxième usager sur ledit réseau de type Internet (RI), ledit deuxième usager étant enregistré sur un
- 5 serveur d'annuaire déterminé (SA_i), en ce que ce dit enregistrement comprend au moins des données dites d'identification dudit deuxième usager, en ce que ladite requête "HTTP" de ladite étape 3/ comprend des premières données indiquant que l'opération demandée est ladite localisation, des deuxième données identifiant ledit deuxième usager à
- 10 localiser et des troisième données permettant d'élaborer, par ladite pièce de logiciel de localisation (A_i), une adresse de type "URL" caractéristique dudit serveur d'annuaire déterminé (SA_i), et en ce que des données identifiant ledit deuxième usager sont transmises, pendant ladite étape 4/ à ce serveur d'annuaire (SA_i), de manière à réaliser ladite localisation
- 15 dudit deuxième usager, par la recherche d'une adresse de type "IP", en associant lesdites données d'identification de ce deuxième usager, reçues par ledit serveur d'annuaire (SA_i), à des données d'enregistrement stockées dans celui-ci, et la retransmission de ladite adresse de type "IP" à ladite carte à puce (2a), de manière à permettre ladite localisation.
- 20
11. Carte à puce destinée à coopérer avec un terminal muni d'un lecteur de carte à puce, pour la mise en relation d'un premier usager avec au moins un serveur d'annuaire, en vue de son enregistrement et/ou de la localisation d'au moins un deuxième usager sur un réseau notamment de
- 25 type Internet, à l'aide de protocoles d'enregistrement et/ou de localisation déterminés, caractérisé en ce que ladite carte à puce (2a) stocke au moins une pièce de logiciel (A_e , A_i) associée aux dits protocoles déterminés d'enregistrement et de localisation, en ce que cette carte à puce (2a)) comporte une pièce de logiciel (23a), formant une couche protocolaire de communication spécifique, comprenant en outre au moins
- 30 une première entité logicielle autonome (S_1), de type dit client et une

44

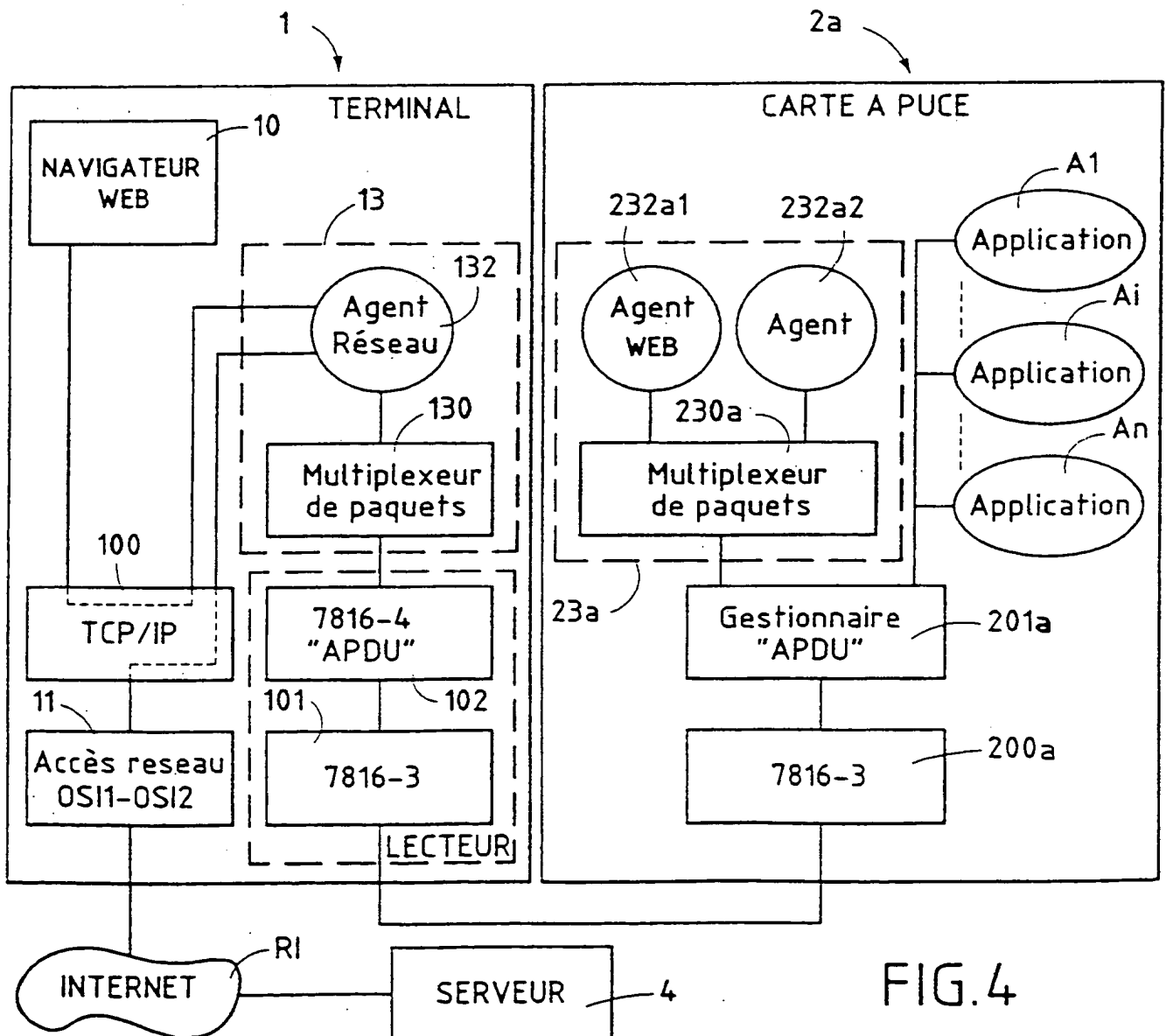
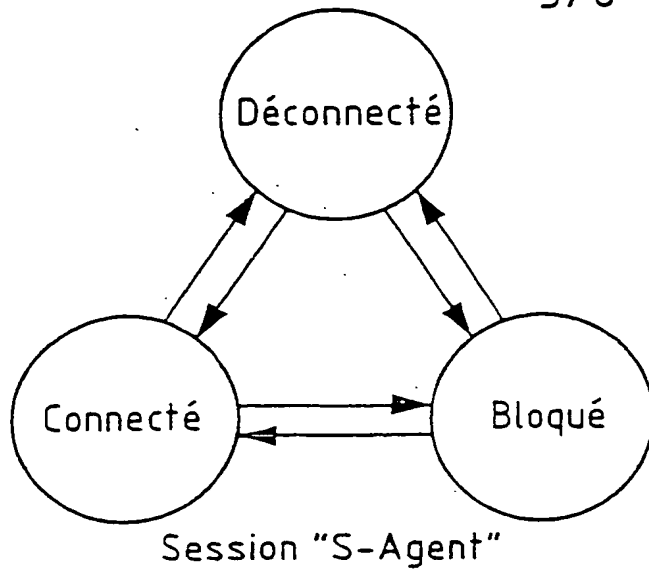
deuxième entité logicielle autonome (S_2), de type dit serveur, lesdites entités (S_2 , S_2) coopérant de manière à ce que ladite carte à puce (2a) offre la fonctionnalité d'un client/serveur de type "WEB" et à permettre ladite mise en relation d'un premier usager avec au moins un serveur d'annuaire (SA_i), via ledit réseau de type Internet (RI), et en ce que ladite carte à puce (2a) comprend au moins une deuxième entité logicielle (AT_e , AT_i) coopérant avec ladite pièce de logiciel spécifique (23a), pour que ladite carte à puce (2a) offre une fonctionnalité d'interface passerelle dite "CGI" permettant l'exécution desdites pièces de logiciel (A_e , A_i) associées aux dits protocoles déterminés d'enregistrement et de localisation.

12. Carte à puce selon la revendication 11, caractérisé en ce que ledit enregistrement s'effectuant à l'aide de données dites de profil d'abonné, décrivant des caractéristiques associées aux dits abonnés, au moins un jeu de données de profil d'abonnés (PA_2) est stocké dans ladite carte à puce (2a).





3/6



4/6

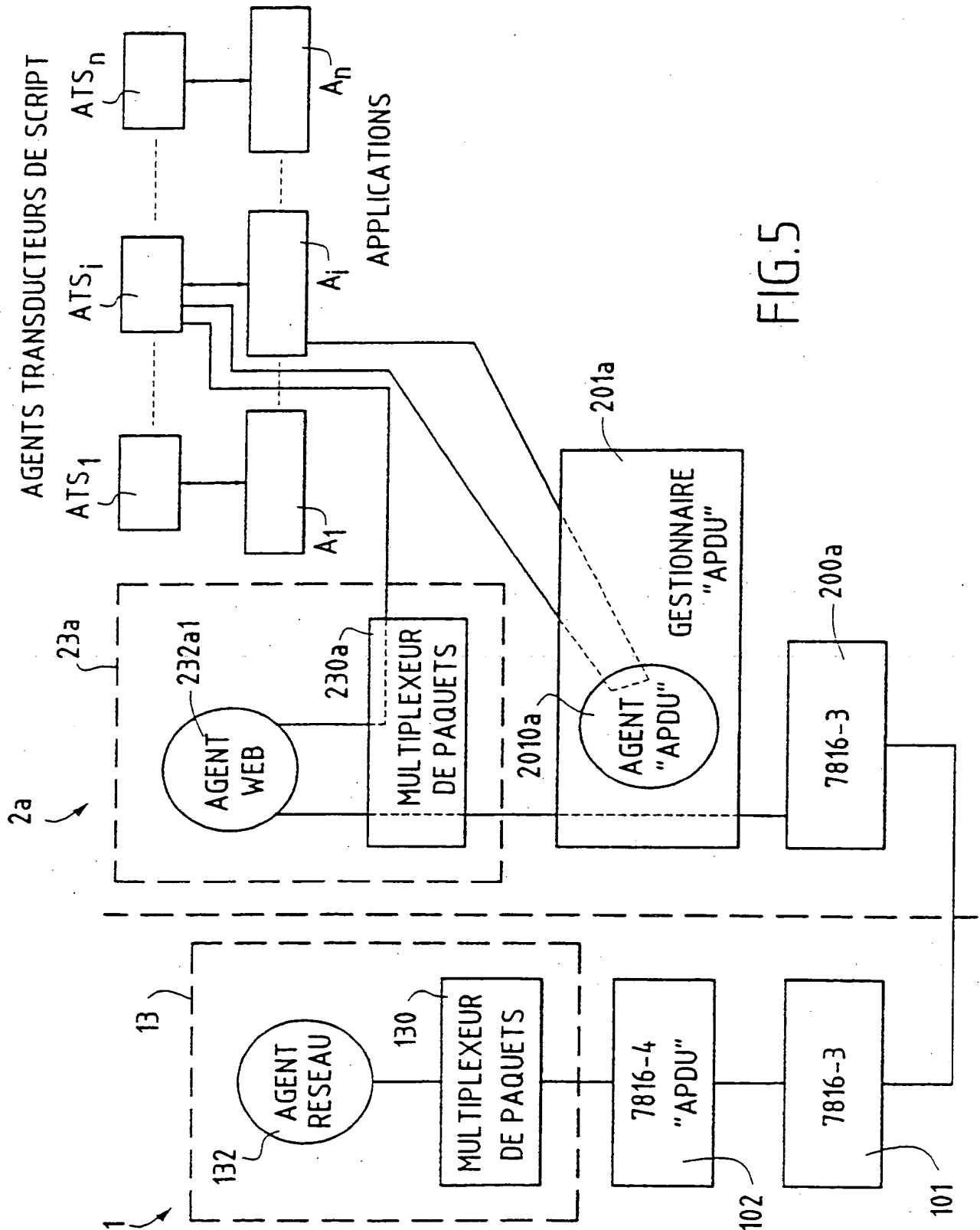
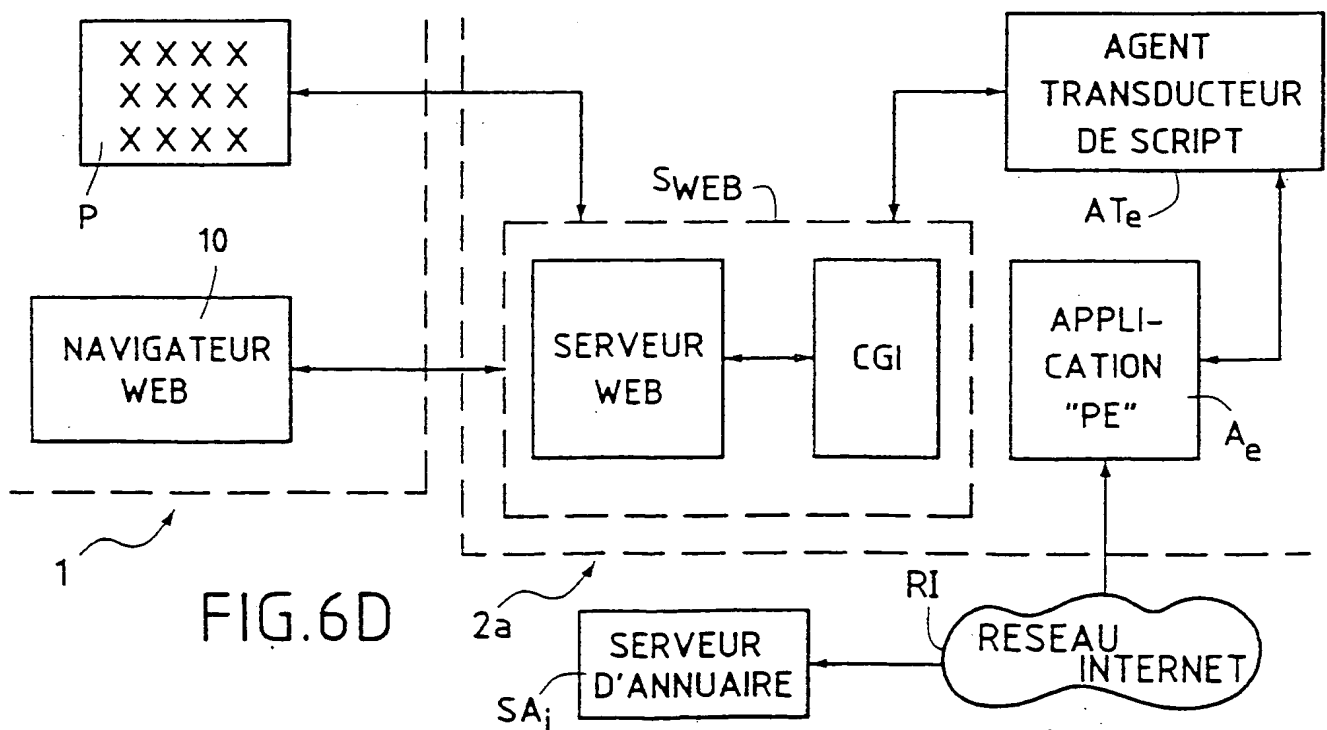
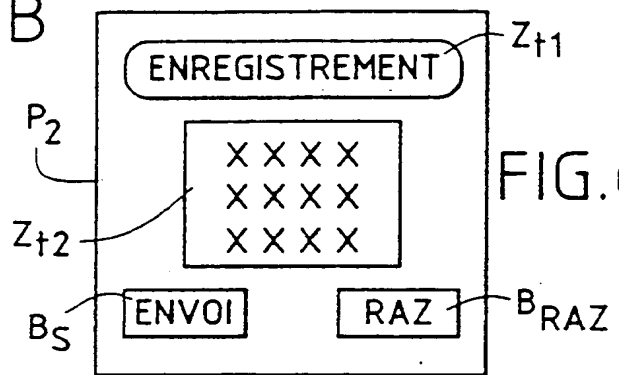
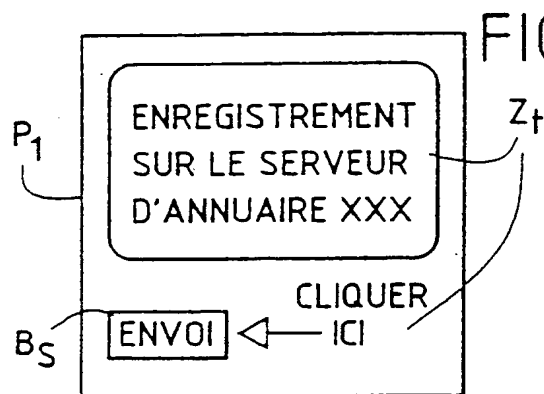
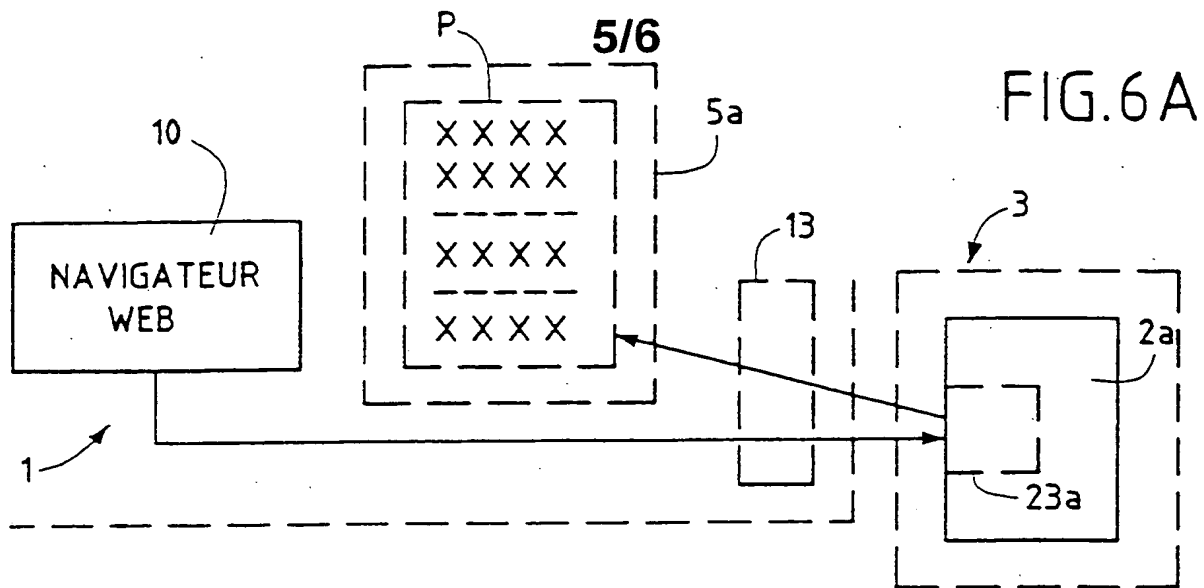


FIG. 5



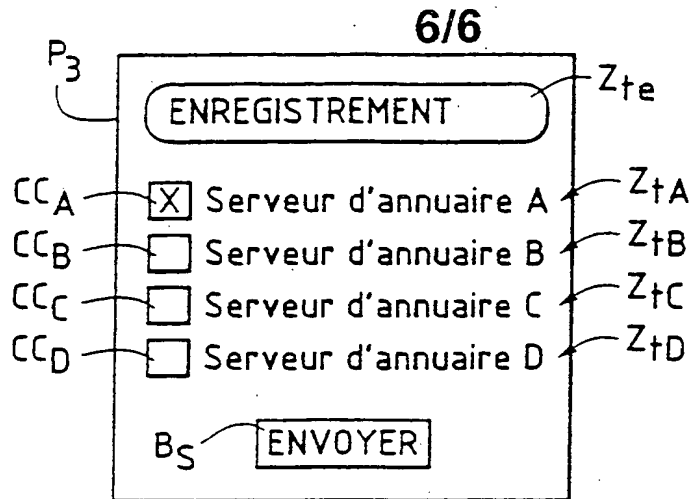


FIG.6E

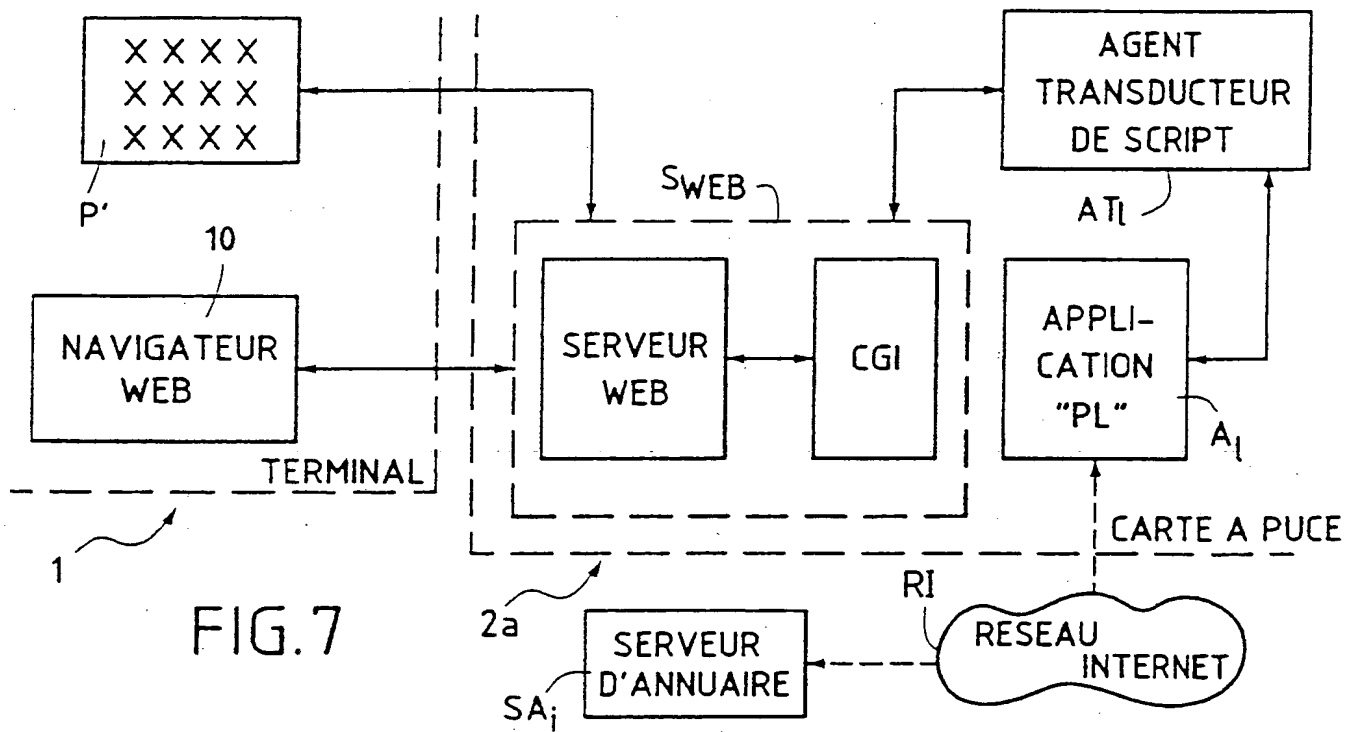


FIG.7

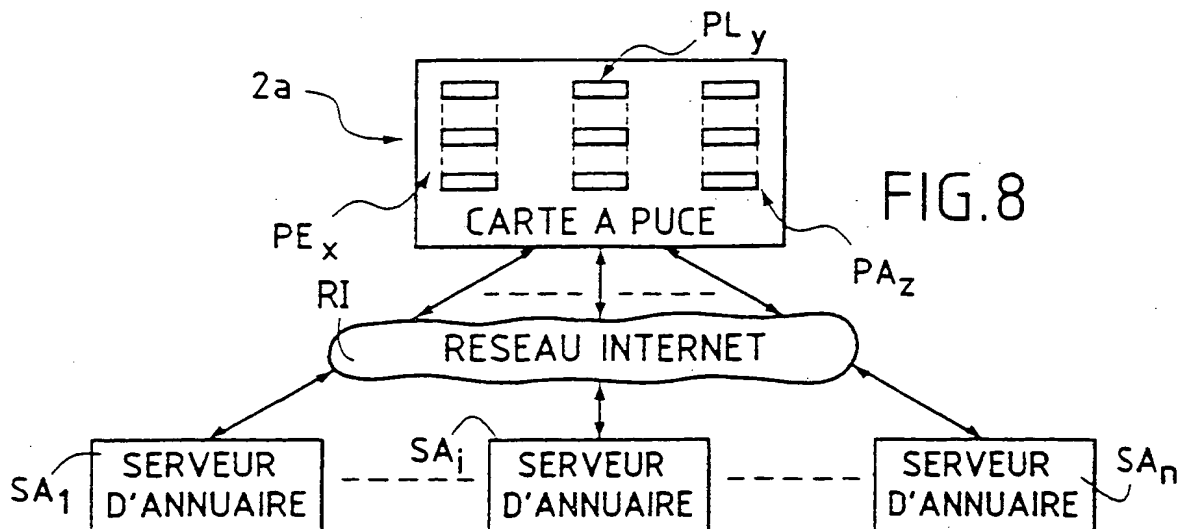


FIG.8

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 01/00396

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/12 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98 57474 A (GEMPLUS CARD INT ; MARTINEAU PHILIPPE (FR); MERRIEN LIONEL (US); SI) 17 December 1998 (1998-12-17) abstract page 1, line 4-10 page 5, line 2 -page 14, line 19 page 16, line 18 -page 23, line 4 ----- -/--	1, 11

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

° Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *&* document member of the same patent family

Date of the actual completion of the international search

10 July 2001

Date of mailing of the international search report

17/07/2001

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040. Tx. 31 651 epo nl.
Fax: (+31-70) 340-3016

Authorized officer

Lievens, K

INTERNATIONAL SEARCH REPORT

International Application No

PC1/FR 01/00396

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>MACAIRE A ; CARLIER D: " A personal naming and directory service for UMTS users" SIXTH INTERNATIONAL CONFERENCE ON INTELLIGENCE IN SERVICES AND NETWORKS, April 1999 (1999-04), page 250-262 XP000961507 Barcelona abstract page 251, line 6 -page 253, line 20 page 255, line 24 -page 257, line 10 figures 1-4</p> <p>-----</p>	1,11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 01/00396

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9857474 A	17-12-1998	AU 8113798 A	30-12-1998
		CN 1284230 T	14-02-2001
		EP 1050145 A	08-11-2000
		TW 378308 B	01-01-2000
		ZA 9805151 A	13-04-1999
<hr/>			

RAPPORT DE RECHERCHE INTERNATIONALE

Der le Internationale No

PCI/FR 01/00396

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L29/12 H04L29/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>WO 98 57474 A (GEMPLUS CARD INT ; MARTINEAU PHILIPPE (FR); MERRIEN LIONEL (US); SI) 17 décembre 1998. (1998-12-17) abrégé page 1, ligne 4-10 page 5, ligne 2 -page 14, ligne 19 page 16, ligne 18 -page 23, ligne 4 ----- -/--</p>	1,11

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- *A* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- *E* document antérieur, mais publié à la date de dépôt international ou après cette date
- *L* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- *O* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- *P* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- *T* document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- *X* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- *Y* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- *S* document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

10 juillet 2001

Date d'expédition du présent rapport de recherche internationale

17/07/2001

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040. Tx. 31 651 epo nl.
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Lievens, K

RAPPORT DE RECHERCHE INTERNATIONALE

Dem. le Internationale No

PCI/FR 01/00396

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>MACAIRE A ; CARLIER D: " A personal naming and directory service for UMTS users"</p> <p>SIXTH INTERNATIONAL CONFERENCE ON INTELLIGENCE IN SERVICES AND NETWORKS, avril 1999 (1999-04), page 250-262</p> <p>XP000961507</p> <p>Barcelona</p> <p>abrégé</p> <p>page 251, ligne 6 -page 253, ligne 20</p> <p>page 255, ligne 24 -page 257, ligne 10</p> <p>figures 1-4</p> <p>-----</p>	1,11

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs à : membres de familles de brevets

Dem. de Internationale No

PCI/FR 01/00396

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9857474 A	17-12-1998	AU 8113798 A	30-12-1998
		CN 1284230 T	14-02-2001
		EP 1050145 A	08-11-2000
		TW 378308 B	01-01-2000
		ZA 9805151 A	13-04-1999
